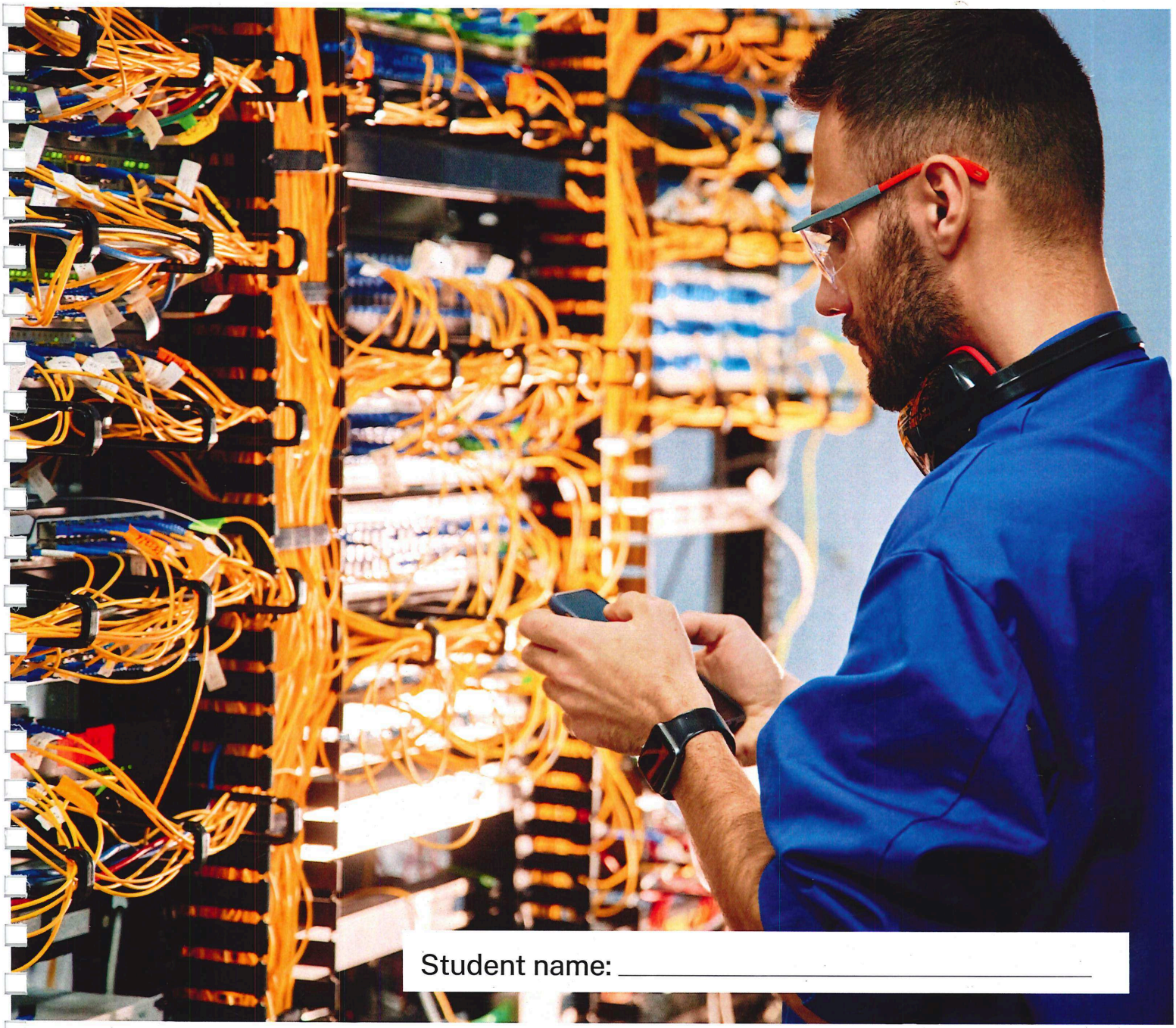
TAFE NSW

Setup and configure basic networks



Student name: _____

tafensw.edu.au

Student Workbook

CONTENTS

Introduction
Other resources
Module organiser

Assessment Guidelines
How you will be assessed
What you need to demonstrate to gain competency

Module Sections

Section 1: Local Area Network Concepts
Review Questions
Practical Exercise 1A

Section 2: LAN Hardware and Cabling
Review Questions
Practical Exercise 2A

Section 3: LAN Protocols and the medium access, OSI Model
Review Questions
Practical Exercise 3A

Section 4 Network Operating Systems and LAN Administration
Review Questions
Practical Exercise 4A

Section 5: LAN Installation
Review Questions
Practical Exercise 5A

Section 6 LAN Interconnectivity
Review Questions
Practical Exercise 6A

Section 7 LAN Trouble Shooting
Review Questions
Practical Exercise 7A

Section 8 Wireless LAN's
Review Questions
Practical Exercise 8

Total time for subject 36 hours

Introduction

This subject, UEECS0029 Setup and Configure Basic Local Area Networks (LAN), is a nationally accredited competency and forms part of the EE-OZ Electronics and Communications stream in the UEE20 Electrotechnology Training Package. There are two formal prerequisite for this unit of competency, UEECS0003 Assemble setup and test computing devices and UEECD0007 Workplace Health and Safety. These units are delivered concurrently during the course.

Assessment

There will be two theory test and one practical assessment. You must pass both theory and practical events as well as demonstrate that you can complete the majority of practical tasks in workbook.

Useful Texts

Andrews, J., *A+ Guide to Managing and Maintaining Your PC*, (Latest Edition), International Thomas Publishing.

Minasi, M., *The Complete PC Upgrade and Maintenance Guide*. (Latest Edition), Sybex.

Mueller, Scott, *Upgrading and Repairing PCs*.. (Latest Edition), Que Corporation.

Text Book

All references in this workbook refer to:

Andrews, J., A+ Guide to *Managing and Maintaining Your PC*, (7th Ed.) International Thomas Publishing.

Reference chapter headings are provided to facilitate using other textbooks.

Other Resources

The best way to keep up-to-date with the continual advancement in computer hardware is by reading computing journals, magazines and subscribing to online tech services over the internet.

Section 1 Local Area Network (LAN) Concepts

Purpose To understand the basic concepts of a Local Area Network.

Objectives At the end of this section you should be able to:

- Describe the purpose of a LAN
- Know the difference between a Peer to Peer LAN and a Server Based LAN
- Describe the different Topologies used in LAN's
- List components required in a LAN
- Know the benefits of a LAN

Reading The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 17 & 18
-
-
-

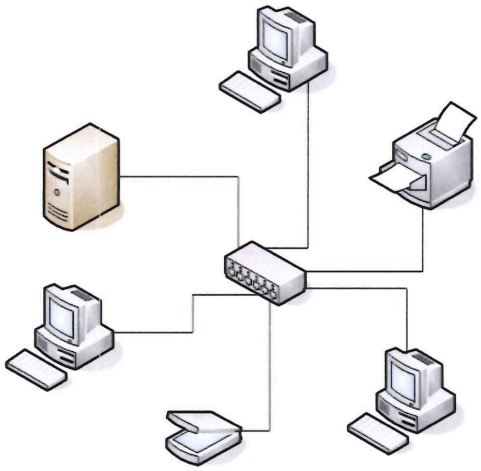
Content

- Purpose of a LAN
- Peer to Peer
- Server Based
- LAN Topologies
- Practical tasks

Not to be reproduced without permission

General Principles of a Local Area Network (LAN)

Definition



Simply defined, a network is a group of computers and other peripheral devices (such as printers) that are connected by some type of transmission media, usually wire or cable or a radio signal. There are infinite variations on the types of hardware, software, transmission media, and designs that make up a network.

Networks may consist of two computers connected by a cable or wirelessly in a home or thousands of computers connected across the world via a combination of cable, phone lines, broadband and satellite links. As well as connecting personal desktop computers and laptops, networks may link together mainframe computers, routers, DVD-Rom's, storage devices, printers, plotters, scanners, USB devices, security cameras, VOIP telephones, smart phones etc. They may transfer information through copper wires, fiber-optic cable, radio waves, or satellite links.

Advantages

Networks offer many advantages relative to a standalone computer. Most importantly, networks enable multiple users to share devices and data. This sharing is referred to as "sharing the networks resources". An organisation that shares devices/resources saves money. Eg: Rather than buying 20 printers for 20 staff members, you can buy one printer and have those 20 staff members share it over a network. Sharing devices also saves time, before networks, transferring data was done via floppy disks.

Another advantage to networks is that they allow you to manage, or administer, hardware and software on multiple computers from one central location. Networks, along with network management software, allow you to manage computers in your office or around the world from one computer.

A computer which you are actually using is referred to as the **local computer**. The computer that you are controlling or working on via the network, is referred to as the **remote computer**. The sharing of devices and the administering of

Not to be reproduced without permission

computers centrally will increase productivity. It's not surprising, then, that most businesses depend on their networks to stay competitive.

Types of Networks

Peer to Peer network

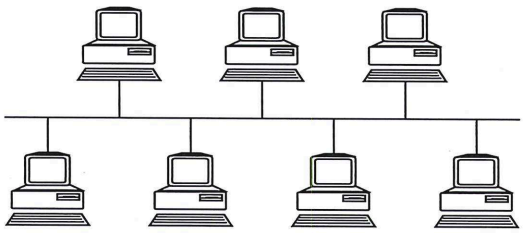


Figure 1-1 A simple peer-to-peer network using bus topology

The simplest type of a network is a **peer-to-peer network**. In a peer-to-peer network, computers communicate directly with other computers on a single segment of cable and share each other's data and devices, such as printers or DVD drives. By default, no computer in a peer-to-peer network has more authority than another. Every computer can use resources from every other computer if sharing is setup on each PC. Most computers in a peer-to-peer network are general-purpose personal computers that are not designed to handle heavy processing loads. These types of networks are known as Workgroups or Homegroups.

Advantages of peer to peer networking

- The primary advantage to using peer-to-peer networks is that they are simple to configure. For this reason, they are often used in environments where there is not a lot of technical expertise.

- Peer-to-peer networks are also less expensive to set up and maintain than other types of networks. This fact makes them suitable for small business and homes where saving money is critical.

Disadvantages of peer to peer networking

- Peer-to-peer networks are not very secure, meaning that data and other resources shared by network users can be easily discovered and used by unauthorized people.

Not to be reproduced without permission

- Traditional peer-to-peer networks are not practical for connecting more than a handful of computers, as they do not necessarily centralize resources. This is because most operators store their own files on their computer and not in a central location, this can cause a problem if someone is looking for a file, as it could be located on more than one machine but as a different version.

- Backup is also a problem as all computers need to backup independently, not a centralised location such as a file server.

Peer to Peer Operating Systems

A peer-to-peer network is set up by configuring Windows 10 or 11 file sharing controls. Peer-to-peer networks do not require a special network operating system (NOS) such as Microsoft Windows Server 2025 , Linux Server. Instead, they use features that are built into their desktop operating system. Each user on this type of network can modify the properties of this operating system to allow others to read and edit files on a particular computer's hard disk. As access depends on many different users, it typically isn't uniform and may not be secure. A user may also mark their printer as a shared printer and allow other users to print to it.

Peer-to-peer network are usually located in a small office or in a home.

Figure 1-2 Simple home network with internet connection

Server Based Networks or Client Server Network

Server-based network, utilise special computers, known as **servers**, computers that connect to a server are known as **clients**. Clients usually take the form of desktop computers, laptops or other mobile devices, these are referred to as **workstations**. A client/server network enables clients to share data, data storage space, and devices.

The server's main job is to allow these clients to share resources. The server must be running a network operating system (NOS), such as Microsoft Windows Server 2022 or 2025, Open Enterprise Server, UNIX or Linux. (By contrast, a standalone computer, or a client computer (workstation), uses a simpler operating system, such as, Windows 10 or 11, MAC OSX versions 14 or 15, or one of many versions of Linux.

A network operating system (NOS) is designed to manage data and other resources on a server for a number of clients. Network operating systems also give the administrator the ability to manage network security, network users and groups, user rights and preferences, protocols, and networked applications.

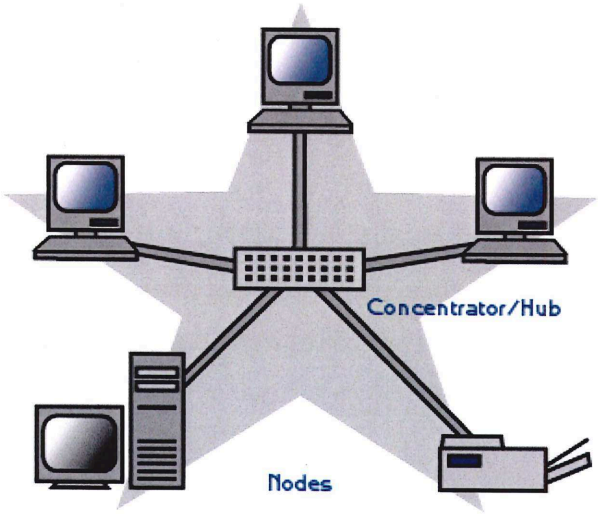


Figure 1-3 A simple server based LAN using star topology

Clients on a network are still able to run applications from and save data to their local hard disk; a server, on the other hand, uses shared applications and data. Typically, clients on a client/server network do not communicate directly with each other but rather use the server as an intermediate step in communications. Servers are usually more powerful computers than workstation computers.

Not to be reproduced without permission

Advantages

Some advantages of *server-based networks* relative to peer-to-peer networks are

- User login accounts and passwords for anyone on a server-based network can be assigned in one place.
- Access to multiple shared resources (such as data files or printers) can be centrally granted, by a single user or groups of users
- Servers are optimized to handle heavy processing loads and dedicated to handling
- Central backup of data

Components required for a simple LAN

The following is a list of components required for a simple wired peer to peer LAN

- Network interface card (NIC)
- Cable (Cat 5 or 6) UTP with RJ-45 modular connectors.
- Switch (Hub) or a connectivity device such as Wi-Fi
- Network capable operating system eg: Window 10 Home, Windows 11 Home
- Suitable PC's

LAN Topologies

The LAN **topology** is the physical layout, or pattern, of the nodes on a network. Physical topologies are divided in three fundamental geometric shapes: bus, star and ring. These shapes can be mixed to create hybrid topologies.

Bus (now obsolete)

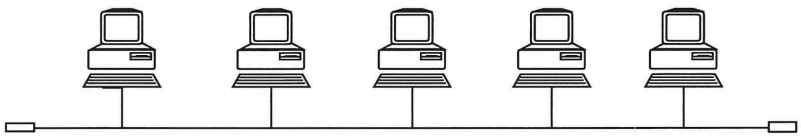


Figure 1-4 Bus topology

A **bus topology** consists of a single coaxial cable connecting all nodes on a network without the use of hubs or connectivity devices.

The single cable is called the **bus** and can support only one channel for communication; as a result, every node shares the bus's total capacity. Most bus networks use coaxial cable as their physical medium. This cable is known as either Thinnet or Thicknet. At each end of the bus is a 50 ohm terminator A bus topology can be considered a peer-to-peer topology, because every device on the network shares the responsibility for getting data from one point to another.
Although networks based on a bus topology are inexpensive to set up, they do not scale well. As you add more nodes, the network's performance degrades. Because of the single channel limitation, the more nodes on a bus network, the more slowly the network will transmit and deliver data. Bus topology is rarely used now days.

Star Topology (most common)

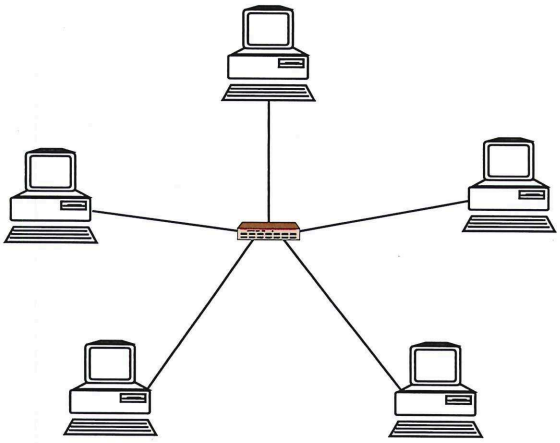


Figure 1-5 A simple Star topology

With a **star topology**, every node on the network is connected through a central device, such as a network switch. Star topologies usually use twisted-pair or fiber optic cabling. Any single cable on a star network connects only two devices, such as a workstation and a hub, so a cabling problem will affect two nodes at most. Devices such as workstations or printers transmit data to the network switch, which then retransmits the signal to the network segment containing the destination node. Star topologies require more cabling than ring or bus networks. However, because each node is separately connected to a central connectivity device, they are more fault-tolerant.

Not to be reproduced without permission

A single malfunctioning cable or workstation cannot disable star networks. A failure of the hub, can stop a LAN segment from working.

As star topology networks include a centralised connection point, they can easily be moved, isolated, or interconnected with other networks; they are therefore scalable. For this reason, and because of their fault tolerance, the star topology has become the most popular layout used in present day LANs. Single star networks are commonly interconnected with other networks through hubs and switches to form more complex topologies.

Ring Topology (also obsolete)

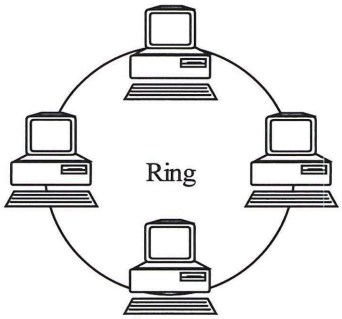


Figure 1-6 Ring Topology

In **ring topology** a node uses the nodes on each side to connect to. This forms a circle or a ring when the entire network is joined. All nodes need to be connected to the ring for the network to work. Data is transmitted clockwise, around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring. In most ring networks, twisted-pair or fiber optic cabling is used as the physical medium. One method for passing data on a ring network is token passing.(More in later weeks) In addition, just as in a bus topology, the more workstations that must participate in token passing, the slower the response time. Consequently, pure ring topologies are not very flexible or scalable.

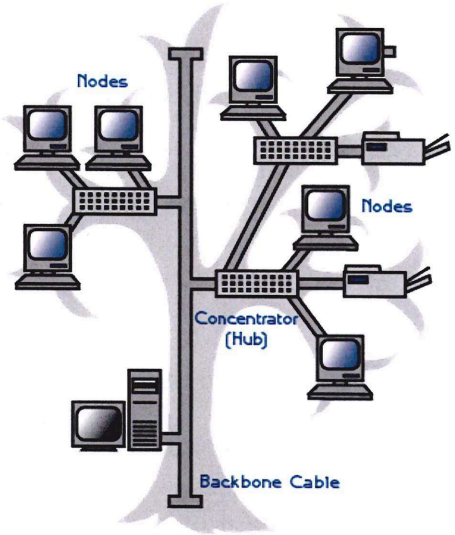
Not to be reproduced without permission

Tree topology

A tree topology combines characteristics of *linear bus and star topologies*. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network and enable business to configure a network to meet their needs.

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Highly scalable by adding branches.
- Reliable – Faults can be easily isolated without effecting the root node.
- Supported by several hardware and software venders.



Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line (root) breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.
- More costly than other networks.

Hybrid topology

A Hybrid network is made up of different types of topology.

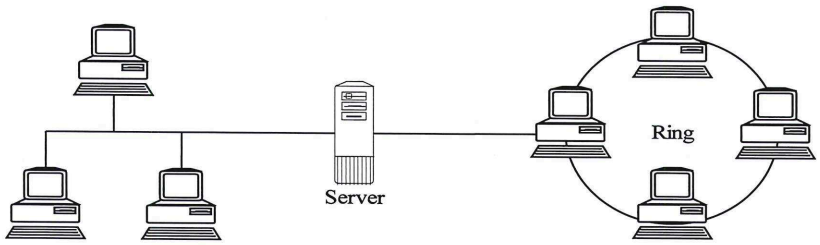
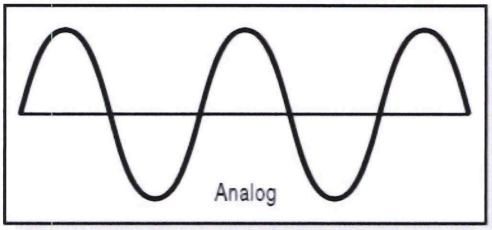


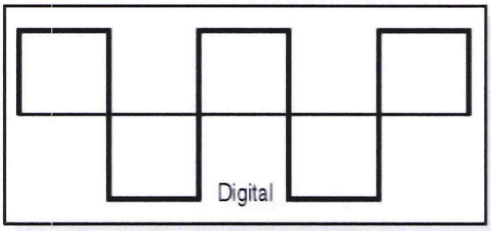
Figure1-8 A **Hybrid** network using Bus and ring Topology

Analogue & Digital Signals



In general, there are two types of telecommunication transmission--Analogue transmission and Digital transmission.

Analogue Transmission



Analog signals are a continuous electrical wave that is an exact replica of a sound wave or picture being transmitted. Signals can be of varying frequency and/or amplitude.

For example, in analog transmission, such as an older telephone system, an electric current of the reproduction of patterned sound waves is transmitted through a wire and into the telephone receiver. Once this is completed, they are then converted back into sound waves.

Digital Transmission

In digital transmission the signals are converted into a binary code, which consists of two elements—positive and non-positive. Morse code and the "on and off" flashing of a light are basic examples. Positive is expressed as the number 1, while non-positive is expressed as the number 0. Numbers that are expressed as a string of 0s and 1s are called binary numbers. In a standard code used by most computers, the letter "A" is expressed in 8 bits as 01000001.

Digital format is ideal for electronic communication as the string of 1s and 0s can be transmitted by a series of "on/off" signals represented by pulses of electricity or light. A pulse "on" can represent a 1 and the lack of a pulse "off" can represent a 0. Information in this form is very much easier to store electronically. Furthermore, digital transmission is usually faster and involves less noise and disturbances as compared to analog data transmission.

Broadband and Baseband

Baseband

Baseband is a form of transmission in which signals are sent through wires. Baseband systems can only transmit one signal at a time or one channel at a time. Each device on a baseband system shares a single channel.

Broadband

A form of transmission in which signals are modulated using radio frequencies with different frequency ranges. This enables several users to send data down the transmission line at the same time. It uses several channels and therefore enables more data to be carried when compared to baseband.
Some broadband signals can suffer from latency (delay).

Not to be reproduced without permission

Review Questions:

1. List 5 types of hardware that can be shared on a network

_____

_____

_____

_____

_____

2. What is the main advantage of using a LAN?

_____

_____

_____

3. What is the difference between a local computer and a remote computer?

_____

_____

_____

4. What is a Peer to Peer Network?

_____

_____

_____

5. Name 3 disadvantages of a peer to peer network

_____

_____

_____

6. Name two advantages of a peer to peer network

_____

_____

Not to be reproduced without permission

7. Describe what a server based LAN is?

_____

_____

_____

8. What is a client?

_____

_____

9. Describe the 3 different LAN Topologies

_____

_____

_____

10. What are 3 advantages of a server based LAN?

_____

_____

_____

11. What type of transmission signal is used in a wired LAN?

_____

_____

_____

12. What is the difference between Baseband and Broadband?

_____

_____

_____

Not to be reproduced without permission

Skill Practice 1-A

To examine the layout of a local area network.

Task

< ***To identify and list the hardware used in the classroom LAN***

Equipment

- Functional computer with Windows 7 or Windows 10 installed.
- An operating network

Procedure

Sketch the cabling layout for the classroom and identify the type of topology.

Classroom LAN:

1. What kind of topology does the classroom LAN use?

_____

Not to be reproduced without permission

Skill Practice 1-B

To examine the operation of a local area network using Win 7 or Win 10

Task

- ***To log on to and out of your classroom LAN***
- ***To use the network copy and transfer a file from one PC to another***
- ***To use the LAN to retrieve a document from a remote PC, modify it using a word processor and return it to the remote PC.***

Equipment

- Functional computer with Windows 7 or Win 10 installed.
- An operating network

Procedure

1. Boot your PC to display desktop,

   Double click on Network (Win7) icon. If there are no network icons on desktop they can be added by personalizing display properties.

Win 10

- Your desktop icons may be hidden. To view them, right-click the desktop, select **View,** and then select **Show desktop icons**. To add icons to your desktop such as This PC, Recycle Bin and more:
- Select the **Start** Windows logo Start button button, and then select **Settings** Gear-shaped Settings icon > **Personalization** > **Themes**.
- Under Themes > Related Settings, select **Desktop icon settings**.

Choose the icons you would like to have on your desktop, then select **Apply** and **OK**

Win 7/10 shows networked PC's as Computers

Can you see any other PC's listed. _____

If you can't call your teacher.

2. From Computer/explorer make a new folder on your C:\ drive called "prac". If this folder already exists delete it and start again.

Win 7- Right click on Folder and select "Share with" – Specific people – click down arrow next to Add – select Everyone then click Add. Change permission to Read/Write. Click Share.

Win 10 Right click on Folder and select : Give access to – Specific people – select dropdown arrow - select Everyone then click Add - Change permission to Read/Write. Click Share.

3. Go back into Network, Click your computer name - can you see a shared folder called Prac.

_____

4. Use Notepad to create a short text file and save it in your "prac" folder. Call it your first name. Type Notepad in search to find it.
5. Using Windows explorer copy this file into the "prac" folder on another workstation in your workgroup.
6. Examine the "prac" folder on the remote PC to make sure the file is there.

7. Delete both of the files (the one on the local PC as well as the remote).

8. Repeat step 4, but this time save it directly to the remote workstations "prac" folder. Delete this file when finished.

Observations

1. What is the difference between saving a file on your local PC and saving it over the network?

_____

2. What does is it mean when you don't tick the box Read/Write (Win 7,10,11)?

_____

_____

3. Use control panel and open up the network connections icon. What information is contained in this folder?

Skill Practice 1-C

Copy a file from a network PC and install it on your PC.

Task

- ***To create a folder on your PC to store a file***
- ***To use the network to copy and transfer a file from one PC to another***

Equipment

- Functional computer with Windows 7 or Win 10 installed.
- An operating network

Procedure

1. Boot your PC. Open Windows Explorer or Computer and create a new folder called Network Stuff. Then go to Network (Win 7,10,11) in explorer.
2. Click on the shared "LANS" folder on the machine indicated by the teacher.
3. Copy the file indicated by the teacher to your Network Stuff folder.
4. Double click on the copied file to install it.

Student Notes:

Section 2 LAN Hardware and Cabling

Purpose

In this section you will learn about the different types of cables that are used to connect the nodes in a LAN. You will also learn the advantages and disadvantages of each cable type.

You will also learn the internationally accepted standard that is used to connect a LAN.

Objectives

At the end of this section you should be able to:

- Describe the following standards 10BaseT, 100BaseT, 100BaseF
- State the relevant advantages and applications of different types of transmission medium
- Cable errors- Crosstalk, attenuation, propagation and skew delay
- Know uses of fibre optic cable

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapters 17 & 18
-

Not to be reproduced without permission

Protocols

A network protocol is a set of rules that governs how a network communicates. A protocol will define the standards for communications between network devices. The main protocols used for networking are come under the IEEE 802.x standards (Institute of Electrical & Electronic Engineers) and include the :

IEEE 802.3 Ethernet standard

IEEE 802.11 Wireless standard

IEEE 802.15 Wireless PAN (personal area network)

TCP/IP, NetBIOS, IPX/SPX, and Apple talk are other protocols which are used in conjunction with the IEEE 802.x standards.

The protocol selected for your network will depend on many factors including the current protocol used on a network, the network operating system, network security, geography of office, technical expertise of users and speed requirements.

Cable Types

Some factors to consider when selecting cable types.

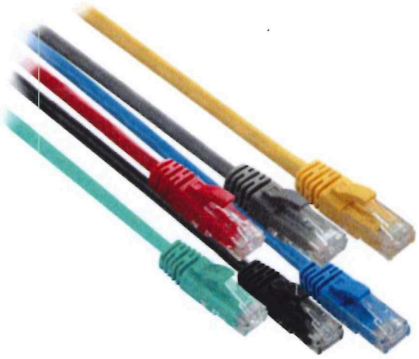
Size and Scalability

When designing your network there are three specifications used to determine the size and scalability of your networking cable.

- Maximum number of nodes per segment
- Maximum length of each segment
- Total maximum length of the network.

Different types of cable will produce different results depending on the physical characteristics of the cable. The maximum number of nodes per segment depends on the amount of signal loss or attenuation. Each device you add to a network segment will slightly increases the signal's attenuation.

TWISTED-PAIR CABLE

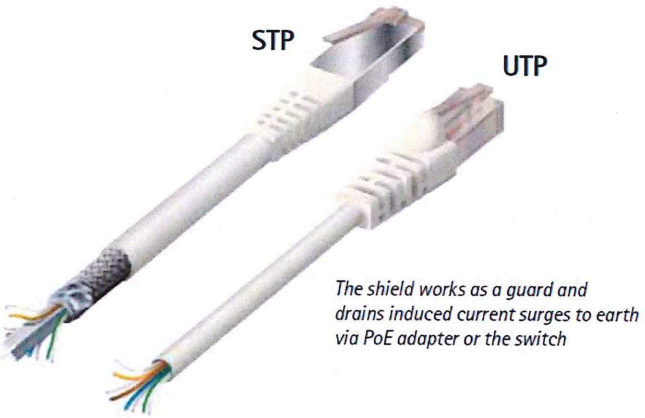


Twisted-pair (TP) cable is similar to telephone wiring and the most common consists of 4 colour-coded pairs of insulated copper wires. The wires are twisted around each other to form pairs and all the pairs are encased in a plastic sheath. The twists in the wire help to reduce the effects of crosstalk. **Crosstalk**, occurs when signals traveling on nearby wire pairs infringe on another pair's signal. Because

they are twisted around each other, the release of current from one wire cancels out the release of current from the adjacent wire. The more twists in a pair of wires, the more resistant the pair will be to all forms of noise. Higher-quality, more expensive twisted-pair cable contains more twists per meter. The number of twists per meter is known as the **twist ratio**. A high twist ratio can result in greater attenuation (loss of signal strength). For optimal performance, cable manufacturers must strike a balance between crosstalk and attenuation reduction. As UTP is used for a variety of purposes, it comes in hundreds of different designs. These designs vary in their twist ratio, the number of wire pairs that they contain, the grade of copper used, the type of shielding (if any), and the materials used for shielding.

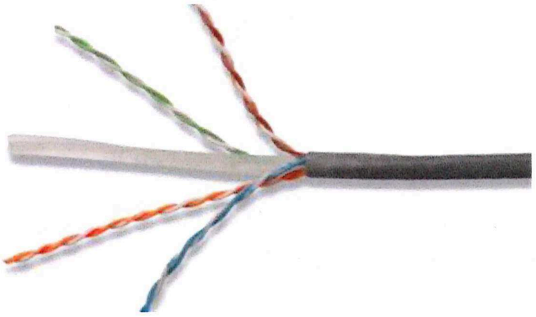
The TIA/EIA 568 standard divides twisted-pair wiring into several categories. These are referred to as CAT (category) 1, 2, 3, 4, 5, 6, and now, CAT 7 and CAT 8. Modern LANs most frequently use CAT 5e or higher wiring. Twisted-pair cable is the most common form of cabling found on LANs today.

Twisted pair cable comes as either unshielded (UTP) or shielded (STP) cable.



Unshielded Twisted-Pair (UTP)

Unshielded twisted-pair (UTP) cabling consists of one or more insulated wire pairs encased in a plastic *sheath*. As its name implies, UTP does not contain additional shielding for the twisted pairs.

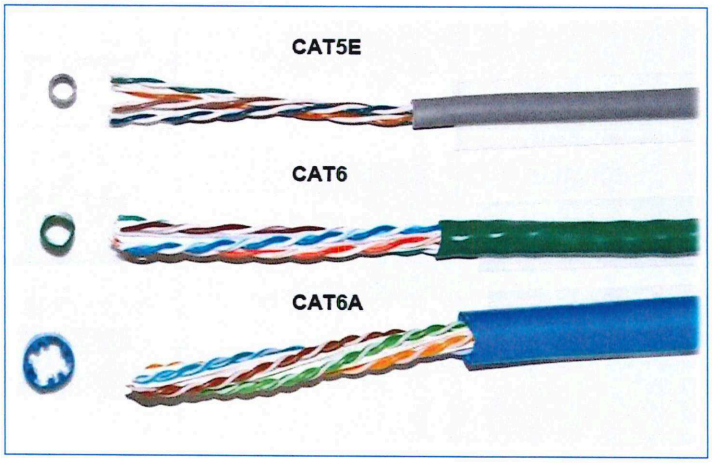


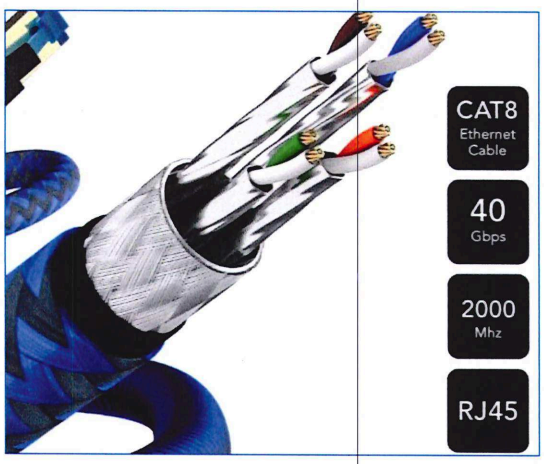
Cat 6 UTP cable with separator

Category	*Older Categories of UTP cables (rarely used any more)*
CAT1	A form of UTP that contains two wire pairs. CAT1 is suitable for voice communications but not for data. With advanced signaling techniques, it can carry up to 128 kilobits per second (Kbps) of data.
CAT2	A form of UTP that contains four wire pairs and can carry up to 4 Mbps of data. CAT2 is rarely found on modern networks, because most systems require higher throughput
CAT3	A form of UTP that contains four wire pairs and can carry up to 10 Mbps of data with a possible bandwidth of 16 MHz. CAT3 was typically used for 10 Mbps Ethernet and 4 Mbps Token Ring networks.
CAT4	A form of UTP that contains four wire pairs and can support up to 16 Mbps throughput. CAT4 may be used for 16 Mbps Token Ring or 10 Mbps Ethernet networks. It is guaranteed for signals as high as 20 MHz and provides more protection against crosstalk and attenuation than CAT1, CAT2, or CAT3.

Category	*Current Categories*
CAT5	Was the most popular form of UTP for network installations and upgrades to Fast Ethernet. CAT5 contains four wire pairs and supports up to 100 Mbps throughput and a 100 MHz signal rate. In addition to 100 Mbps Ethernet, CAT5 wiring can support other fast networking technologies. Note: 100MHz/100Mbps/100m. No longer used.
CAT5e	A higher-grade version of CAT5 wiring that contains high-quality copper, offers a high twist ratio, which reduces crosstalk. Enhanced CAT5 can support a signaling rate as high as 200 MHz, double the capability of regular CAT5, Note: 100-250MHz/1Gbps/100m.
CAT6	A twisted-pair cable that contains four wire pairs, each separated from each other. The separated pairs provide excellent resistance to crosstalk and enables CAT6 to support 250MHz bandwidth or at least six times the throughput supported by regular CAT5. Most newly installed networks now use CAT6. Note: 500MHz/10Gbps/100m

CAT6a	Shielded UTP cable suitable for 500MHz Bandwidth and speeds up to 10Gbps. Note: 500MHz/10Gbps/100m.
CAT7	A twisted-pair cable that contains multiple wire pairs, each surrounded by its own shielding, then packaged in additional shielding beneath the jacket. One advantage to CAT7 cabling is that it can support signal rates up to 1 Ghz. However, it requires different connectors than other versions of UTP because its twisted pairs must be more isolated from each other to ward off crosstalk. Because of its added shielding, CAT7 cabling is also larger and less flexible than other versions of UTP cable. CAT7 is rare on current networks Note: 600MHz/10Gbps/100m (40Gbps at 50m).
CAT 8 ***Latest***	Is the latest IEEE standard in copper Ethernet cable. The Cat8 Ethernet cable can eliminate crosstalk and enable higher data transmission speeds by wrapping each twisted pair in foil. Cat8 cable can support 25GBASE-T and 40GBASE-T Ethernet, which can be used in data centers, high-speed and bandwidth-intensive places. Thus, the Cat8 cable is more expensive than previous generations of Ethernet cable. Note: 2000MHz/25Gbps for Cat8.1 and 40Gbps for Cat8.2.





Figures 2-3 UTP Cable types. Note, twist ratio. Cat 8 cable braid and foul shielding

The performance of different Ethernet cable categories from Cat5 to Cat8 is as follows:

Category	Transmission Speed	Transmission Distance	Bandwidth	Shielding Type	Application
Cat5	100Mbps	100m (328ft.)	100MHz	Unshielded	100BaseT Ethernet
Cat5e	1Gbps	100m (328ft.)	100MHz	Unshielded	Gigabit Ethernet, residential homes
Cat6	1/10Gbps	100m (328ft.) 10Gb at 37-55m (121ft.)	250MHz	Shield/Unshielded	Gigabit Ethernet, commercial buildings
Cat6a	10Gbps	100m (328ft.)	500MHz	Shield/Unshielded	Gigabit Ethernet, data centres, and commercial buildings
Cat7	10Gbps	100m (328ft.)	600MHz	Shield	10Gbps core infrastructure
Cat8	25/40Gbps	30m (98ft.)	2000MHz	Shield	25/40Gbps core infrastructure

Standards - 10BASE-T, 100BASE-T and 1000BASE-T,

Definition - what does “10, 100, and 1000”, “BASE” and “T” , “F” mean?

The "**10**" "**100**" "**1000**" in the media type designation refers to the transmission speed of 10,100, 1000 Mbps, they represents the frequency in MHz (Mega HertZ) for which this cable is made. They represent for 10MHz, 100 MHz, and 1000 MHz. The greater the MHz, the greater speeds the cable can handle.

Not to be reproduced without permission

The "**BASE**" refers to baseband signaling, which means that only Ethernet signals are carried on the medium. (Through repeaters, media segments of different physical types can be sometimes be used in the same system.)

The "**T**" refers to "Twisted Pair" physical medium that carries the signal. This shows the structure of the cable and tells us it contains pairs which are twisted. "F" is Fibre Optic.

Informal name	Common name	Formal IEEE name	Speed	Cable & Max Length	Suitable Cable
10 BASE-T	Ethernet	802.3	10Mbps	Copper,100 m	Category 5
100 BASE-T	Fast Ethernet	802.3u	100Mbps	Copper,100 m	Category 5e
1000 BASE-T	Gig Ethernet	802.3z	1000Mbps	Copper,100m	Category 6
100 BASE-FX	Fast Ethernet	802.3u	100Mbps	Fiber,2000m	Multimode

Cable Characteristics and Errors

Crosstalk

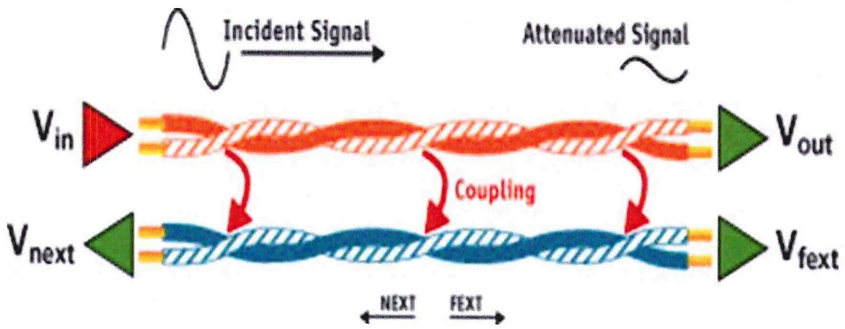


Fig: Attenuation and cross talk

Whether its coaxial cable, or UTP, copper-based cabling is susceptible to crosstalk. Crosstalk happens when the signal from one cable gets mixed up with the signal in another cable. This can happen when cables run too closely together or are not terminated correctly. Some cables use shielding to help reduce the impact of crosstalk. As network speeds increase so does incidents of crosstalk and other errors.

Near-End Crosstalk (NEXT)

NEXT refers to interference between adjacent wire pairs within the twisted-pair cable at the near-end of the link (the end closest to the origin of the data signal). NEXT occurs when an outgoing data transmission leaks over to an incoming transmission. In effect, the incoming transmission overhears the signal sent by a transmitting station at the near end of the link. The result is that a portion of the outgoing signal is coupled back into the received signal and corrupts the data.

Not to be reproduced without permission

Far-End Crosstalk (FEXT)

FEXT occurs when a receiving station overhears a data signal sent by a transmitting station at the other end of a transmission line. FEXT identifies the interference of a signal through a wire pair to an adjacent pair at the farthest end from the interfering source (the end where the signal is received).

Electromagnetic interference (EMI)

Electromagnetic interference (EMI) can change signals or corrupt them altogether. EMI occurs when cables are run too close to everyday office fixtures such as computer CRT monitors, fluorescent lighting fixtures, elevators, microwaves, and anything else that creates an electromagnetic field. Again, the solution is to carefully run cables away from such devices. If they have to be run through EMI areas, shielded cabling or fibre cabling needs to be used. A balanced UTP cable helps eliminate the effects of EMI. EMI will slow a network down as it causes damaged packets of data to be transmitted.

Attenuation

All transmission media have recommended lengths that the cable can be run. This is because data signals weaken as they travel farther from the point of origin. If the signal travels far enough, it can weaken so much that it becomes unusable. The weakening of data signals as they pass through the media is referred to as attenuation. All copper based cable is particularity susceptible to attenuation. When cable lengths have to be run farther than the recommended lengths, signal regenerators (network switch) can boost the signal as it travels. If you work on a network with intermittent problems and notice that cable lengths run too far, attenuation can be the problem.

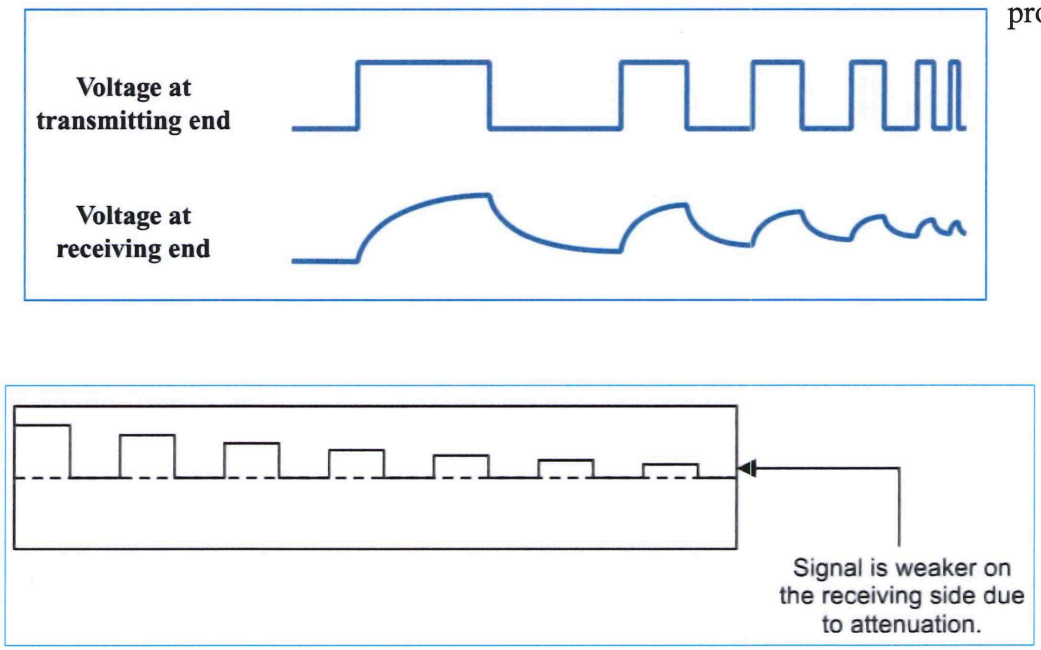


Fig: Attenuation

Propagation Delay and Delay Skew

Delay is a property that is known to exist for all types of transmission media. The propagation delay is equivalent to the amount of time that passes between when a signal is transmitted and when it is received on the other end of a cabling channel. The effect is similar to the delay in time between when lightning strikes and thunder is heard-except that electrical signals travel much faster than sound. The actual delay value for twisted-pair cabling is a function of the *Nominal Velocity of Propagation* (NVP), length and frequency.

NVP varies according to the dielectric materials used in the cable and is expressed as a percentage of the speed of light. For example, most category 5 cables have NVP ranges from 0.65c to 0.70c (where "c" represents the speed of light ~299,000 Km/s) when measured on finished cable.

Lower NVP values will contribute to additional delay for a given length of cable, just as an increase in end-to-end cable length will cause a proportionate increase in the end-to-end delay. As with most other transmission parameters, delay values are frequency dependent. Normal propagation delay of up to 570 ns/100m doesn't cause a problem in a LAN.

Nominal velocity of propagation (NVP)

- NVP refers to how quickly signals travel in a cable expressed as a percentage relative to the speed of light in vacuum

$$NVP = \frac{\text{speed at which pulse travels in cable}}{\text{speed of light in vacuum}} \times 100\%$$

Delay Skew

When multiple pairs in the same cable exhibit different delay performance, the result is delay skew. Delay skew is determined by measuring the difference between the pair with the least delay and the pair with the most delay. Factors that affect delay skew performance include material selection, such as conductor insulation, and physical design, such as differences in twist rates from pair to pair.

Propagation delay and delay skew performance are specified by some local area network (LAN) standards for worst case 100 m channel configurations to ensure proper signal transmission. Transmission problems associated with excessive delay and delay skew include increased jitter and bit error rates.

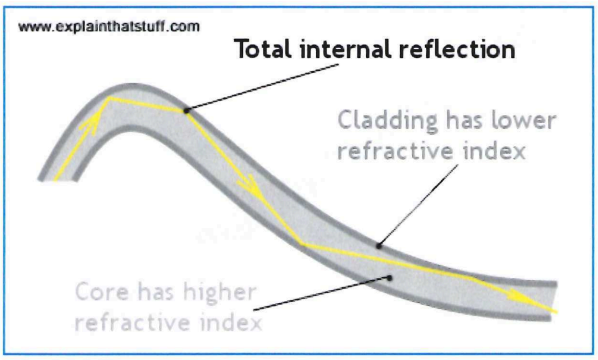
Based on IEEE 802-series LAN specifications, a maximum propagation delay of 570 ns/100m at 1 MHz and a maximum delay skew of 45ns/100m up to 100 MHz are recommended for TIA category 5, 4-pair cables.

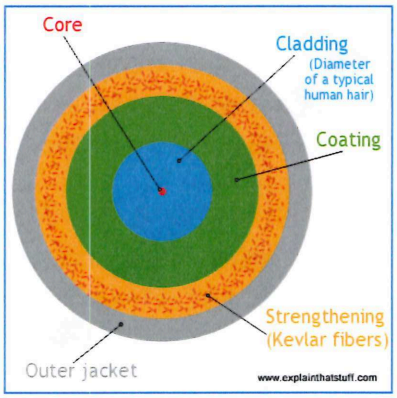
Although propagation delay and delay skew are noteworthy, it is important to note that the most significant cabling performance issue for most LAN applications remains to be attenuation to crosstalk ratio (ACR).

Not to be reproduced without permission

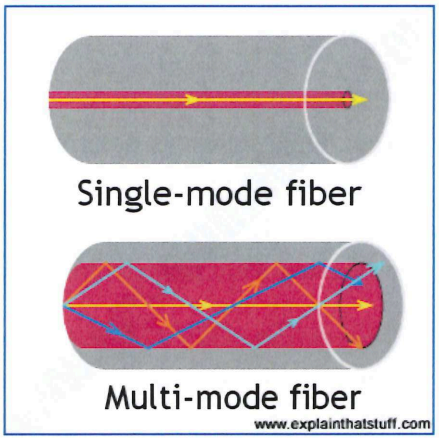
FIBRE-OPTIC CABLE

Fibre-optic cable, or simply *fiber*, contains one or several glass fibers (or polymer) at its center or **core**. Data is transmitted by either a pulsing light sent from a laser or light-emitting diode (LED) through the central fibers. Surrounding the fibers is a layer of glass or polymer called **cladding.** The cladding glass is a different density from the glass in the strands. It acts as a mirror, reflecting light back to the core. This reflection allows the fiber to bend around corners without diminishing the integrity of the light-based signal.





There are two categories of fibre: single-mode and multimode.



Single-mode fiber uses a narrow core (less than 10 microns in diameter) through which light generated by a laser travels over one path, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows single mode fiber to accommodate high bandwidths and long distances (without requiring repeaters). Single-mode fiber may be used to connect a carrier's two facilities. However, it costs too much to be considered for use on typical data networks.

Multimode fibre contains a core with a larger diameter than single-mode fiber (between 50 and 100 microns in diameter) over which many pulses of light generated by a light emitting diode (LED) travel at different angles. Because light is being reflected many different ways in a multimode fiber cable, the waves become less easily distinguishable the longer they travel. Thus, multimode fiber is best suited for shorter distances than single-mode fiber. It is commonly found on cables that connect a router to a switch or a server on the backbone of a network.

Fiber-optic cable provides the benefits of nearly unlimited throughput and very high resistance to noise. Fiber can also carry signals for longer distances than can coax or twisted-pair cable. Finally, fiber is widely accepted by the high-speed networking industry. The most significant

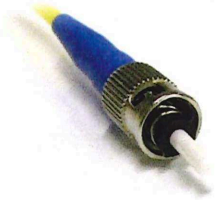
Not to be reproduced without permission

drawback to the use of fiber is its high cost. Another disadvantage is that fiber can transmit data in only one direction at a time; to overcome this drawback, each cable must contain two strands—one to send data and one to receive it. Finally, unlike copper wiring, fiber is difficult to splice and time consuming, special tools and equipment are required to splice cables. Fiber's characteristics are summarized as follows.

Throughput (Speed)	Exceeding 1000 Mb's
Segment length	See below
Maximum network length	See below
Maximum number of segments	6
Number of nodes per segment	1024
Connectors	ST ,LC or SC connectors
Additional hardware	Hubs or Switches ,NIC's with ST or SC
Noise immunity	Immune to EMI & RFI noise
Cost	Expensive

COMMON FIBRE OPTIC LENGTHS

10BaseFL (Multimode fibre)
Length: 2000m or 2km

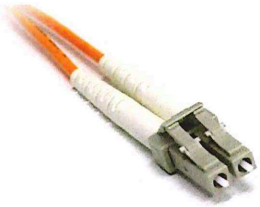


100BaseFX Half-duplex (Multimode fibre)
Length: 412m

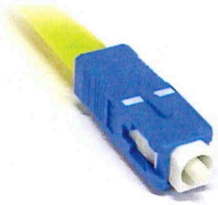
ST Connector

100BaseFX Full-duplex (Multimode fibre)
Length: 2000m or 2km

100BaseFX Full-Duplex ONLY (Single mode fibre)
Length: 2-40,000m or 2-40km *(see note)



1000Base-LX
Length: 550m (62.5 or 50 multimode fibre)
3000m (10 single mode fibre)



LC Connector

1000Base-SX
Length: 250m (62.5 multimode fibre)

Not to be reproduced without permission

550m (50 multimode fibre)

1000Base-ZX
Length: Approx 70 km uses single mode fibre at 1550 nm wavelength

SC Connector

***NOTE:** These lengths can vary by equipment vendor. Some products will enable 100Mbps Full Duplex over 100km. There are many other different types of fibre cables

Wireless LAN

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, lasers or microwaves to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission (needs line of site), or by satellite.

Wireless networks are great for allowing laptop computers or other remote devices to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables. Wireless networks now connect to Smart phones, touch pads, tablets and other devices.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from electrical and electronic devices. They are also slower than LANs using cabling and have a limited distance that they can transmit and receive. See section 8 for more detailed information on Wireless LAN's

PIC: Diagram of a typical wireless network

REVIEW QUESTIONS:

1. When they become faint, analog signals are regenerated while digital signals are amplified. True or False?

2. How does electrical "noise" affect a digital signal?

a. Noise enhances a digital signal.

b. Noise weakens a digital signal.

c. Noise distorts the signal.

d. Noise does not affect digital signals.

3. Which of the following would not be a source of EMI?

a. fluorescent lighting

b. a loud gong

c. a cord that carries electricity to a printer

d. a lightning storm

4. What is the term that refers to the outermost covering of a cable?

a. cladding

b. insulation

c. plenum

d. sheath

e. braiding

5. What are two advantages of using shielded twisted-pair STP cabling over unshielded UTP cabling on a network?

a. Unshielded Twisted-pair cable is more reliable.

b. Shielded Twisted-pair cable is less expensive.

c. Shielded Twisted-pair cable is more resistant to noise.

d. Unshielded Twisted-pair cable is more resistant to physical damage.

e. Shielded Twisted-pair cable is required for faster transmission standards, such as 1000BaseT.

7. In which of the following network types would you use a cable with SC connectors?

Not to be reproduced without permission

a. 10Base5

b. 10Base2

c. 10BaseT

d. 10BaseF

e. 100BaseFX

8. What type of termination is required at both ends of a CAT6 patch cable?

a. SC Connector

b. ST Connector

c. RJ-45 Connector

d. 6 ohm category connector

9. Which three of the following network types use a star topology?

a. 10Base5

b. 10Base2

c. 10BaseT

d. 100BaseTX

e. 100BaseF

10. Crosstalk does not present a problem for UTP cable.

True or False?

11. How many wire pairs are in a typical CAT5e cable?

a. 2

b. 3

c. 4

d. 5

12. What type of fiber-optic cable is most frequently found on LANs?

Not to be reproduced without permission

a. multithreaded fiber

b. twisted fiber

c. single-mode fiber

d. braided fiber

e. multimode fiber

13. Which two of the following are drawbacks to using fiber-optic cable for LANs?

a. It is expensive.

b. It cannot handle high bandwidth transmissions.

c. It can carry transmissions using only the TCP/IP protocol.

d. It can be difficult to install and repair.

e. It is not yet an accepted standard for high-speed networking.

14. What is the maximum segment length on a 100BaseTX network?

a. 10 m

b. 100 m

c. 200 m

d. 400 m

e. 1000 m

15. What is the maximum segment length on a 1000BaseT (gigabit) network?

a. 50 m

b. 100 m

c. 200 m

d. 500 m

e. 1000m

16. On what type of network would you use RJ45 (8P8C) connectors?

Not to be reproduced without permission

a. 10Base5

b. 10Base2

c. 100BaseTX

d. 100BaseFX

17. What is the *maximum* amount you should untwist twisted-pair wires before inserting them into 8P8C connectors?

a. 6 mm

b. 12 mm

c. 18mm

d. 25 mm

e. 44 mm

18. If you wanted to allow two workstations to transmit and receive data between their NICs without using a connectivity device, which of the following would you need?

a. crossover cable

b. straight-through cable

c. AUI cable

d. Multimode cable

Not to be reproduced without permission

Making a crossover cable

Task

To make a crossover patch cable to connect 2 pc's directly.

A Crossover cable can connect 2 PC's together without the need of a network switch.

Equipment needed

- A length of Cat5 cable
- 2 x RJ45 (8P8C) connectors
- Crimping tools and cutters
- Cable tester

Procedure

1. Using the wire cutter, make a clean cut at both ends of the UTP cable.
2. Using the wire stripper, remove the sheath off approximately 25mm off one end of the UTP cable, being careful to not damage the insulation on the twisted pairs inside.
3. Separate the four wire pairs slightly while keeping each pair next to the other.
4. Arrange wires in correct colour order as indicated by table. For a crossover cable you have a 568a and a 568b on each end. Trim back wires so that about 12 mm extends past sheath. Make sure that the wires are cut in a straight line. Check that wires are still in the correct order and insert them into the RJ 45 connector ensuring that they go all the way to the end of connector. Using the crimping tool, crimp the wires in the RJ-45 connector.
5. Repeat Steps 1 through 5 for the other end of the UTP cable making sure you use the other wiring code.
6. Test your cable with the cable tester. Show teacher.

RJ45 Pin	Wire Colour 568A	Wire Diagram 568A	10Base-T Signal 100Base-TX Signal
1	White/Green		Transmit+

Not to be reproduced without permission

RJ45 Pin	Wire Colour 568A	Wire Diagram 568A	10Base-T Signal 100Base-TX Signal
2	Green		Transmit-
3	White/Orange		Receive+
4	Blue		Unused
5	White/Blue		Unused
6	Orange		Receive-
7	White/Brown		Unused
8	Brown		Unused

Table 1: TIA/EIA 568A pinout colour guide looking from smooth side of connector

RJ45 Pin	Wire Colour 568B	Wire Diagram 568B	10Base-T Signal 100Base-TX Signal
1	White/Orange		Transmit+
2	Orange		Transmit-
3	White/Green		Receive+
4	Blue		Unused
5	White/Blue		Unused
6	Green		Receive-
7	White/Brown		Unused
8	Brown		Unused

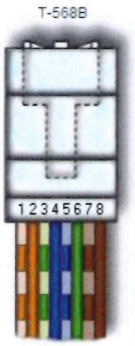


Table 2: TIA/EIA 568B pin out colour guide looking from smooth side of connector

Section 3 OSI Model, LAN Protocols and Medium Access

Purpose

To understand the principles of operation of common LAN protocols and medium access methods.

Objectives

At the end of this section you should be able to:

- Understand the reason why we need internationally accepted standards
- Have an understanding of the OSI model and be able to relate the model to real systems
- Explain the operation of the Ethernet protocol in terms of the IEEE 802.3 standard.
- Explain the operation of common medium access methods

  CSMA/CD

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 18

ISO

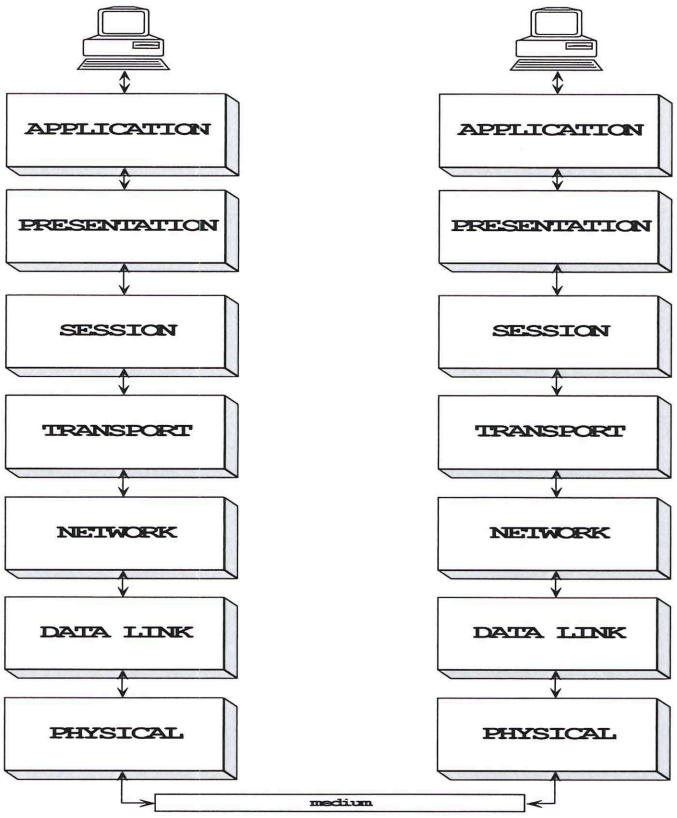
ISO is a network of the national standards institutes of 147 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO (International Organization for Standardization) is the world's largest developer of standards. Although ISO's principal activity is the development of technical standards, ISO standards also have important economic and social repercussions. ISO standards make a positive difference, not just to engineers and manufacturers for whom they solve basic problems in production and distribution, but to society as a whole. The ISO standards enable different manufacturers to develop products that can communicate with a variety of systems. Most network vendors relate their network products to the ISO standard of the OSI model.

OSI

7-layer OSI MODEL

The OSI (Open System Interconnection) model is developed by ISO in 1984 to provide a reference model for the complex aspects related to network communication. It divides the different functions and services provided by network hardware and software into 7 layers. This facilitates modular engineering, simplifies teaching and learning network technologies, helps to isolate problems and allows vendors to focus on just the layer(s) in which their hardware or software is implemented and be able to create products that are compatible, standardized and interoperable.



The diagram shows the 7 layers of the OSI Model, to remember them in the correct order a common mnemonic is often used: In top down order. Eg:

All People Seem To Need Data Processing

The Application, Presentation and Session layer are known as the *Upper Layer* and are implemented in software. The Transport and Network layer are mainly concerned with protocols for delivery and routing of packets to a destination and are implemented in software

as well. The Data Link is implemented in hard- and software and the Physical layer is implemented in hardware only, hence its name.

A more detailed description of each layer follows below, but here's what basically happens when data passes from Host A to Host B:

1. The Application, Presentation and Session layer take user input and converts it into data,
2. The Transport layer adds a segment header converting the data into segments,
3. The Network layer adds a network header and converts the segments into packets / datagrams,
4. The Data Link layer adds a frame header converting the packets / datagrams into frames,
5. The MAC sublayer layer converts the frames into a bits which the Physical layer can put on the wire.

These steps are known as the 5 steps of *data encapsulation*. When the bits stream arrives at the destination, the Physical layer takes it off the wire and converts it into frames, each layer will remove their corresponding header while the data flows up the OSI model until it is converted back to data and presented to the user, this is known as *decapsulation*.

7. APPLICATION

The Application layer provides network services directly to the user's application such as a web browser, email software and Windows Explorer. This layer is said to be "closest to the user". The application layer uses the API (Application program interface) which is a routine (a set of instructions that communicates with the operating system) that is built in to applications such as Microsoft Word to communicate on this layer.
Protocols that operate on this layer include: TELNET, HTTP, FTP, SMTP.

6. PRESENTATION

This layer 'represents' the data in a particular format to the Application layer. It defines encryption, compression, conversion and other coding functions.
Specifications defined at this layer include: GIF, JPEG, MPEG, and ASCII.

5. SESSION

Establishes, maintains and terminates end-to-end connections (sessions) between two applications on two network nodes. It controls the dialogue between the source and destination node, which node can send, when and for how long. Also provides error reporting for the Application, Presentation and Session layer.

Not to be reproduced without permission

Protocols/API's that operate on this layer include: RPC, NETBIOS.

4. TRANSPORT

This layer converts the data received from the upper layers into ***segments***. The Transport layer is responsible for end-to-end (also called source-to-destination) delivery of entire messages. It provides end-to-end connectivity, it allows data to be transferred reliably and sequencing to guarantee that it will be delivered in the same order that it was sent. It provides services such as error checking and flow control (software). Protocols that operate on this layer: TCP, UDP, NETBEUI, SPX.

3. NETWORK

This layer converts the segments from the Transport layer into ***packets*** (or datagrams) and is responsible for path determination, *routing*, and the delivery of these individual packets across multiple networks without guaranteed delivery. The network layer treats these packets independently, without recognizing any relationship between those packets, it relies on upper layers for reliable delivery and sequencing. Also this layer is responsible for *logical addressing* (also known as network addressing or Layer 3 addressing) for example IP addresses Protocols defined at this layer: IP, IPX, ICMP, RIP.
Devices that operate on this layer: Routers, Layer 3 Switches.

2. DATA LINK

The Data Links provides transparent network services to the Network layer so the Network layer can be ignorant about the physical network topology and provides access to the physical networking media. It is responsible for converting data it receives from the network layer and converting it into ***frames***. It will also reassemble bits taken of the wire by the Physical layer to frames, making sure they are in the correct order, it will requests retransmission of frames if an error occurs. It provides error checking by adding a CRC to the frame, and flow control.

Devices that operate on this layer: Switches and Bridges.
The Data Link layer is divided into 2 sub layers.

IEEE 802 DATA LINK sub layers

The IEEE refined the standards and divided the Data Link layer into two sub layers: the LLC and the MAC sub layer.

LLC sub layer - LLC is short for Logical Link Control. The Logical Link Control is the upper sub layer of the Data Link layer. LLC masks the underlying network technology by hiding their differences hence providing a single interface to the

network layer. This helps the lower layers communicate to the Network layer protocols acting as an intermediate between the different network protocols (IPX, TCP/IP, etc.) and the different network types (Ethernet, Token Ring, etc.) This layer is also responsible for frames sequencing and acknowledgments.

MAC sub layer

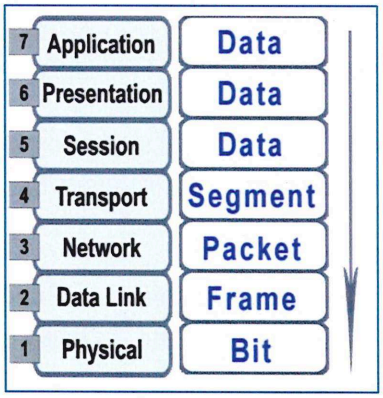
The Media Access Control layer takes care of physical addressing and allows upper layers access to the physical media, handles frame addressing, error checking. This layer controls and communicates directly with the physical network media through the network interface card. It converts the frames into bits to pass them on to the Physical layer who puts them on the wire (and vice versa).

1. PHYSICAL

This layer communicates directly with the physical media, it is responsible for activating, maintaining and deactivating the physical link. It handles the raw ***bit*** stream and places it on the wire to be picked up by the Physical layer at the receiving node. It defines electrical and optical signaling, voltage levels, data transmission rates and distances as well as mechanical specifications such as cable lengths and connectors, the amount of pins and their function. Devices that operate on this layer: HUBs, concentrators, repeaters and NICs.

Summary

Layer	OSI Layer	Function
7	Application	Transfers information from program to program
6	Presentation	Handles text formatting and displays code conversion
5	Session	Establishes, maintains and coordinates communications
4	Transport	Ensures accurate delivery of data
3	Network	Determines transport routes and handles transfer of messages
2	Data Link	Codes, addresses, and transmits information
1	Physical	Manages hardware connections



POPULAR LAN STANDARDS

Ethernet IEEE 802.3

Ethernet is a networking technology originally developed at Xerox in the early 1970s and improved by Digital Equipment Corporation, Intel, and Xerox. Ethernet refers to the way that data is broadcast over the whole network. It is modeled on the satellite protocol called ALOHA in which the satellite transmits a frame of data into the ETHER (space) and ground station listen to see if message is for them. Ethernet is to do with hardware and the type of network card used. It operates in layer 1 and 2.

The basic rules of Ethernet are **CSMA/CD** which is used to minimise the chance that two computers will transmit data on the network at the same time.

1. **CS - Carrier Sense**. The network is monitored for a "carrier", or presence of a transmitting station. This process is known as "**carrier sense**".

2. **MA - Multiple Access**. All stations have same level of access to medium.

3. If an active carrier is detected, then transmission is deferred. The station continues to monitor the network until the carrier ceases.

4. If an active carrier is not detected, and the period of no carrier is equal to or greater than the interframe gap, then the station immediately begins transmission of the frame.

5. While the transmitting station is sending the frame, it monitors the medium for a collision.

6. **/CD - Collision Detection**. If a collision is detected, the transmitting station stops sending the frame data and sends a 32-bit "jam sequence". The sequence jam is transmitted to ensure that the length of the collision is sufficient to be noticed by the other transmitting stations.

7. After sending the jam sequence the transmitting station waits a random period of time chosen using a random number generator before starting the transmission process over from step 1 above. This process is called "**backoff**". The probability of a repeated collision is reduced by having the colliding stations wait a random period of time before retransmitting.

8. If repeated collisions occur, then transmission is repeated, but the random delay is increased with each attempt. This further reduces the probability of another collision.

9. This process repeats until a station transmits a frame without collision. Once a station successfully transmits a frame, it clears the collision counter it uses to increase the backoff time after each repeated collision.

Not to be reproduced without permission

A Typical Ethernet Frame

Preamble	Destination Address	Source Address	Frame Type	Data	FCS/ CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 B

Figure 3-5 depicts a typical Ethernet frame as specified by the IEEE **802.3** standard.

The components of the Ethernet 802.3 frame are described in the following table:

	Description
Preamble	*Marks the beginning of the entire frame, providing a signal that essentially announces to the network that data is en route. Synchronize sequence for NICs.*
Destination Address	*Contains the destination node MAC (Medium Access Control) address.*
Source Address	*Contains the MAC address of the originating node.*
Frame type	*Refers to the format of the data in the frame eg: 8137Hex would indicate that the data frame contained an IPX (OSI level 3 routing protocol) frame, Novell Netware*
Data	*Contains the data, or segmented part of that data, transmitted from the originating node. Always 1500 bytes unless it is last packet. It is padded out to 46 if needed.*
FCS or CRC	*Frame Check Sequence (FCS) Provides an algorithm to determine whether the data was received correctly. The most commonly used algorithm is called* ***Cyclic Redundancy Check (CRC)****, so you may also see this field called "CRC."*

IEEE 802.11 Wireless

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of medium access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires. IEEE 802.11 is also a basis for vehicle-based communication networks with IEEE 802.11p.

The standards are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote the capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard. 802.11x is a shorthand for "any version of 802.11", to avoid confusion with "802.11" used specifically for the original 1997 version.

IEEE 802.11 uses various frequencies including, but not limited to, 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz frequency bands. Although IEEE 802.11 specifications list channels that might be used, the allowed radio frequency spectrum availability varies significantly by regulatory domain.

The protocols are typically used in conjunction with IEEE 802.2, and are designed to interwork seamlessly with Ethernet, and are very often used to carry Internet Protocol traffic.

General description

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The 802.11 protocol family employs carrier-sense multiple access with collision avoidance (CSMA/CA) whereby equipment listens to a channel for other users (including non 802.11 users) before transmitting each frame (some use the term "packet", which may be ambiguous: "frame" is more technically correct).

Wi-Fi generations V·T·E

Generation	IEEE standard	Adopted	Maximum link rate (Mb/s)	Radio frequency (GHz)
(Wi-Fi 0)*	802.11	1997	1–2	2.4
(Wi-Fi 1)*	802.11b	1999	1–11	2.4
(Wi-Fi 2)*	802.11a	1999	6–54	5
(Wi-Fi 3)*	802.11g	2003		2.4
Wi-Fi 4	802.11n	2009	6.5–600	2.4, 5
Wi-Fi 5	802.11ac	2013	6.5–6933	5[a]
Wi-Fi 6	802.11ax	2021	0.4–9608[1]	2.4, 5
Wi-Fi 6E				2.4, 5, 6[b]
Wi-Fi 7	802.11be	exp. 2024	0.4–23,059	2.4, 5, 6[2]
Wi-Fi 8	802.11bn	exp. 2028[3]	100,000[4]	2.4, 5, 6[5]

https://en.wikipedia.org/wiki/IEEE_802.11

Review Questions:

1. What does "ISO" stand for?

    a. Institute for Standards Organization

    b. International Standards Organization

    c. International Organization for Standardization

    d. International Statisticians Organization

2. Which technology is standardised in the IEEE 802.3 specification?

    a. Network security

    b. Token Ring LANs

    c. Wireless networks

    d. Ethernet LANs

3. Which technology is standardised in the IEEE 802.11 specification?

    a. Network security

    b. Token Ring LANs

    c. Wireless networks

    d. Ethernet LANs

4. Which layer of the OSI Model provides file transfer services?

    a. Application layer

    b. Data Link layer

    c. Transport layer

    d. Presentation layer

5. Firefox (web browser) is an example of a program that runs in the Application layer.

    True or False?

Not to be reproduced without permission

6. Which layer of the OSI Model establishes the rules of communication between two nodes?

    a. Transport layer

    b. Session layer

    c. Data Link layer

    d. Presentation layer

7. In which layer of the OSI Model do switches and bridges belong?

    a. Data Link layer

    b. Transport layer

    c. Network layer

    d. Session layer

8. In which layer of the OSI Model do routers belong?

    a. Data Link layer

    b. Transport layer

    c. Network layer

    d. Physical layer

9. In which two layers of the OSI Model do NIC's belong?

    a. Presentation and Application layer

    b. Transport and Network layer

    c. Network and Data Link layer

    d. Physical and Data Link layer

10. Which standards organization developed the OSI Model?

    a. IEEE

    b. ITU

    c. OSI

    d. ISO

Not to be reproduced without permission

12. Which layer of the OSI Model handles error checking and retransmission of bad data?

    a. Transport layer

    b. Network layer

    c. Session layer

    d. Physical layer

13. What are the differences between MAC addresses and Network layer addresses?

_____

_____

14. Token Ring technology was originally developed by which company?

    a. Hewlett-Packard

    b. IBM

    c. Cisco

    d. 3Com

15. How to collisions occur in an Ethernet LAN?

_____

_____

_____

_____

16. What conditions are likely to make collisions greater?

_____

_____

18. What is a CRC or FCS and what is it used for?

_____

_____

Not to be reproduced without permission

19. What does CSMA/CD stand for?

20. Name the seven layers of the OSI model in top down order.

Not to be reproduced without permission

Skill Practice 3A

Exploring Network settings

Task

To familiarise yourself by using a Windows operating system to examine the hardware and software which is used for network operations on your PC.

Equipment

• Functional computer with either Windows **7** or Windows **10** installed. ***Follow appropriate instructions for your operating system.***

Procedure

Boot the computer.

1. **Win 7** - Use Control panel and go to network and sharing center – Click on Change adapter settings then click on local area connection icon and select properties

   Alternate - Right click on Network icon on desktop and follow above steps.

   Win 10 - Right click on Network icon in explorer and select properties.

   Click change adaptor settings – right click on network icon – select properties

2. Record the following information about your network settings.

   Connect using:

   _____

   This connection uses the following items:

   _____

   _____

   _____

   _____

   _____

   _____

   _____

Not to be reproduced without permission

3. Find out your computer identification and which Workgroup it belongs to.

Win 7 - Right click on Computer on desktop, select properties.

Win 10 – Type Workgroup in task bar search box

Record the following information

Computer description: (if applicable)

_____

Full computer name:

_____

Workgroup:

_____

Domain: (If applicable)

_____

Skill Practice 3B

LAN tasks needed to share network resources

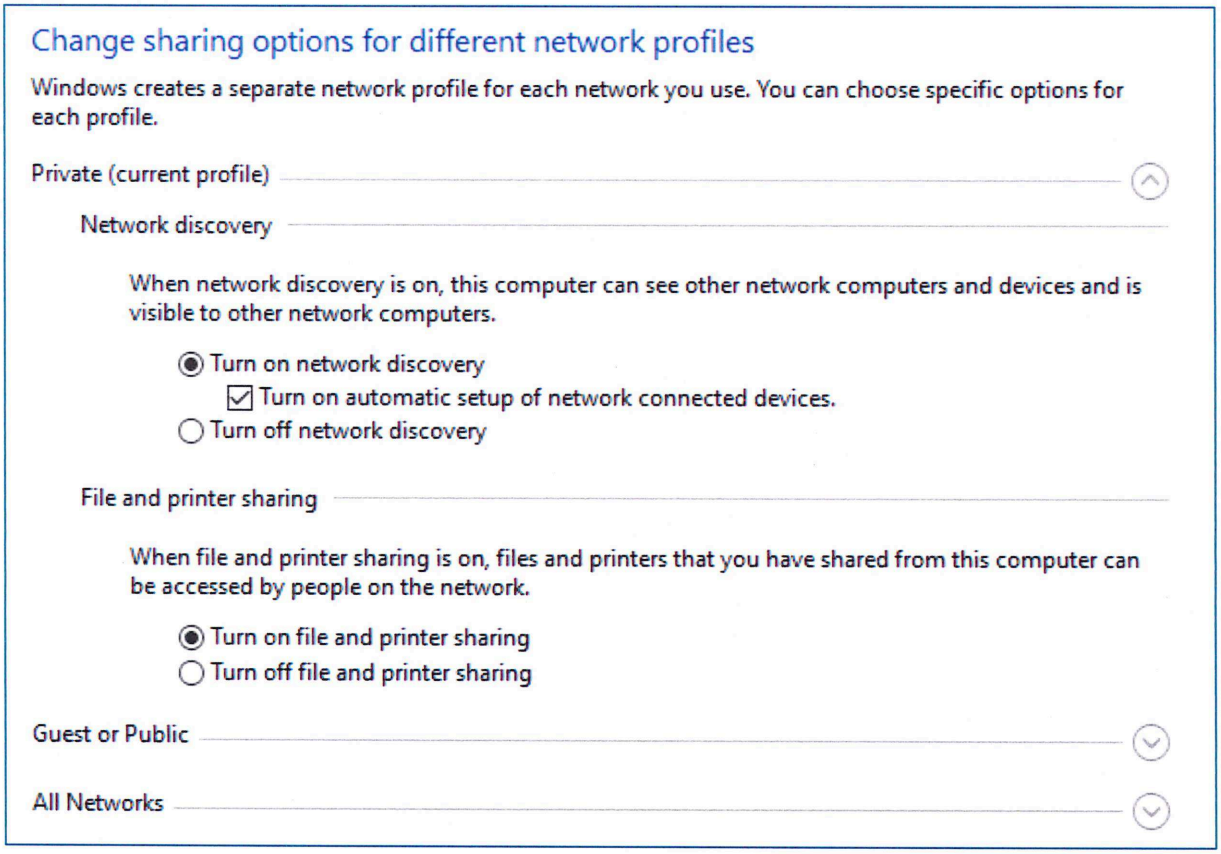
Task - for Windows 8 & 10

To use a Windows operating system to examine the networking tasks available **Procedure**

1. **Win 7 or 10 -** Right click on Network icon in explorer and select properties.

Click - change advanced sharing settings – right click on network icon – select properties

1. Make sure the following are selected



2. Select Guest or Public

Guest or Public

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

- (●) Turn on network discovery
- ( ) Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

- (●) Turn on file and printer sharing
- ( ) Turn off file and printer sharing

3. Select All Networks

All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

- ( ) Turn on sharing so anyone with network access can read and write files in the Public folders
- (●) Turn off Public folder sharing (people logged on to this computer can still access these folders)

File sharing connections

Windows uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

- (●) Use 128-bit encryption to help protect file sharing connections (recommended)
- ( ) Enable file sharing for devices that use 40- or 56-bit encryption

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

- ( ) Turn on password protected sharing
- (●) Turn off password protected sharing

Save Changes

Not to be reproduced without permission

Skill Practice 3C

Task:

To make a shortcut to a network location on a remote PC.

You can use this procedure to create a shortcut to a folder on the local network or a personal online folder located on the Internet or a FTP site on the Internet.

Windows 7

1. Right click on Network icon.
2. Select Map network drive.
3. Select a drive letter eg: M
4. Choose a path to a network location by selecting Browse and locate **Display PC** (or other PC as indicated by Teacher).
5. Select shared folder music. Click OK. The address should display **\\Display\music** (\\ indicates network drive, Display is the remote machine on the network and music is the shared folder we will access).
7. Make sure Reconnect at logon is ticked.
8. Click Finish, The folder will connect and display contents. Close this folder.
9. Go back to the desktop and open Computer, You should see a shortcut to the music folder on the display computer under Network Location. Open folder to display contents.
10. Once done. Delete the folder you created by going back to desktop and right clicking on Network icon and selecting Disconnect Network Drive. Highlight drive with mouse and then press OK.

Not to be reproduced without permission

Skill Practice 3D

Task:

To use a third party software to find IP addresses of other nodes on a network. **Windows 7 and Windows 10.**

Procedure:

1. If Softperfect Network Scanner program is not installed on PC, obtain from either the teacher or download it from http://www.softperfect.com. (Free download). Note: Free version as limited capability.
2. Start program
3. Click on Options/IP range/Detect local IP range.
4. Select IP Range it finds that corresponds to your network address.
5. Click Start Scanning tab
6. Observe results, this could take a few minutes to locate all nodes.

Questions:

1. How many connections did it find?

_____

2. Can you access any shared folders on other computers? Hint click on +.

_____

3. What is the range of response times?

_____

4. Why do you think there is a variation in times?

_____

5. What is an advantage of using this software?

_____

_____

Not to be reproduced without permission

Student Notes:

Not to be reproduced without permission

Section 4

Network Operating Systems & LAN Administration

Purpose

To understand the different types of network operating systems and know their uses.

Objectives

At the end of this section, you should be able to:

- Explain what a NOS is and what components are included
- Concepts of a Windows base Peer to Peer network.
- Use a server base operating system such as Windows 2000
- Compare a Peer to Peer network to a Server Based Network

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 18

Not to be reproduced without permission

Network Operating Systems

There are over 100 different Network Operating Systems (NOS). All versions of Windows can be networked. The most common included:

- Windows Server 2003 to 2025 – 14 versions, based on Windows NT.
- Novell Netware – Very popular in the 90's, Open Enterprise Server
- UNIX – originally a minicomputer OS – used for specialist software
- FreeBDS based around UNIX
- CISCO – UCS - Unified computing system – hardware & software
- LINUX – various versions - some free

Essential software components

Each workstation and server must contain the following.

1. A "program redirector" software Redirector software is used to determine if a request should be handled by the client or by the server. Redirector programs are located in both the client and the server.

2. A **network protocol** is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

   They include

   TCP/IP (Windows, LAN, WAN, Internet) (Most common)

   DHCP (Dynamic Host Configuration Protocol)

   FTP (File transfer protocol)

   UDP (User datagram protocol)

3. The client machine must also contain a client software package such as

   Client for Microsoft Networks, if connected to a Windows network

   Client for Linux Networks, if connecting to a Linux server

Not to be reproduced without permission

PEER to PEER Fundamentals

With a peer to peer network each PC requires

1. A network adaptor card

   An installed driver for card

   An installed operating system such as Win 10 Home or Win 11 Home.

   A connectivity device

2. Each PC is able to operate as a standalone PC or has the option of being able to share its folders and hardware resources and peripherals (eg: printer, DVD-ROM drive) with other users on the network.

3. Each PC must have a unique Computer name and belong to a WORKGROUP or Homegroup (Win 7, 8) Dropped in Win 10 & 11.

4. Use the same network protocol such as TCP/IP.

5. Shared level security is the only level available

6. Any PC can be set up to operate as the "Server"

   - A File Server has common files loaded on its HDD or other storage devices.
   - A Print Server allows all network users access to the shared printer attached to it.
   - A Communication Server will offer connection to external networks such as Internet, WAN's, public telephone networks.

7. As a general rule the most powerful PC will act as the "server" and preferably not used as a workstation. There is a limit to the capability of a single processor.

8. In order for a workstation to use a printer it must have the correct printer driver loaded on it.

Server Based LAN fundamentals

1. Each PC requires the same hardware and network adaptor as a Peer to Peer LAN.

2. The NOS is loaded on the file server with a client version loaded on each workstation. The workstations connect to a Domain.

Not to be reproduced without permission

3. Each workstation may run any version of Windows Pro series with a redirector program suited to the Server Operating System. TCP/IP is the usual protocol.

4. Setting up the network requires the skills of a Certified Network Engineer. (CNE).

5. Maintaining the network requires the skills of a Certified Network Administrator. (CNA).

6. When a workstation is booted up the Microsoft Client displays a log on screen.

7. Once a user has logged on to the network, a range of network resources becomes available.

8. A printer driver must be loaded on to each workstation in order for the workstation to use it.

9. The network administrator can log in from any workstation and modify/control the network. Their responsibilities include:

System security

- Access to folders
- Access to files
- Read/Write abilities in folders
- Limit what the user can "see"

Printing

- To set up print queues
- To assign priorities for users
- To control the print queue

File Management

- To design and organise a directory structure that complies with the NOS standards.
- To maintain system and file backup
- Create log on scripts to enable users to access system with little networking knowledge.

Not to be reproduced without permission

Applications

- Maintain licenses for all application on the network.
- Loads shared applications

Documentation

- All user accounts, groups, permissions, privileges etc, must be documented.
- TCP/IP settings, DNS names etc.
- Printer resources and setting.
- Anything related to network security, software or file management.

NetBIOS

Some network software requires the use of NetBIOS. NetBIOS (Network Basic Input Output System) was originally developed by IBM as an Application Program Interface (API) for client software to access LAN resources. NetBIOS is a layer of software developed to link the network operating system and network hardware such as the NIC by providing a uniform set of commands for requesting lower-level services required to conduct sessions between nodes. NetBIOS has been adopted as an industry standard. NetBIOS uses computer names as a means of identifying computers on the network. NetBIOS operates in the session layer.

Accounts

User Accounts

In Windows Server two types of user accounts are defined:

- **Domain user accounts** Users accounts defined in Active Directory are called *domain user accounts*. Through Single Sign-On, domain user accounts can access resources throughout the domain. Domain user accounts are created in Active Directory Users And Computers.
- **Local user accounts** User accounts defined on a local computer are called *local user accounts*. Local user accounts have access to the local computer only, and they must authenticate themselves before they can access network resources. You create local user accounts with the Local Users and Groups utility.

Not to be reproduced without permission

Groups

Users are added into Groups to make administration easier. You can assign privileges to a group and all users in the group are assigned the same privileges.

Group Types

In Windows Server, there are three types of groups:

- **Domain local groups -** Groups that are defined on a local computer. Local groups are used on the local computer only. You create local groups with the Local Users And Groups utility.
- **Domain global groups -** Groups that are created on a domain controller. They can be put into any Local groups of any machine. They are the most common group. You create local groups with the Local Users and Groups utility.
- **Universal groups -** Groups that are a "do it all" type of group.

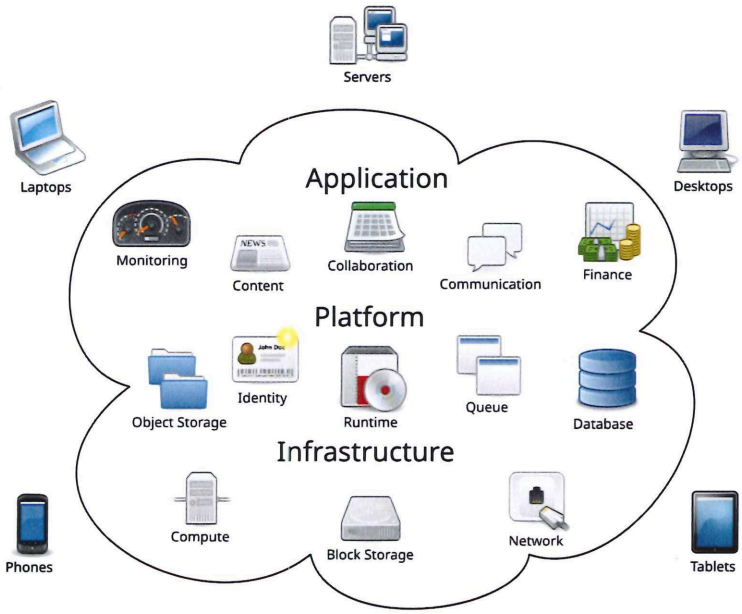
Group types

- **Security groups:** Groups that can have security descriptors associated with them. You define security groups in domains using Active Directory Users and Computers.
- **Distribution groups:** Groups that are used as e-mail distribution lists. They can't have security descriptors associated with them. You define distribution groups in domains using Active Directory Users and Computers.

Cloud Computing

Cloud computing is the use of both hardware and software resources over a network, typically the Internet. The name comes from the cloud shaped symbol that is typically used to show the Internet on network diagrams.

Users access applications through their browser or an app on their mobile device. Their applications and data are stored on the remote server and can be accessed from almost anywhere.



The concept of Cloud computing is not new and has been around since the 1950's when we had mainframe computers and thin clients or terminals. These were just dumb workstations that didn't have any storage capabilities and directly access the server for all functions.

Cloud computing saves the end user purchasing expensive servers, the cost of setup, and ongoing maintenance costs. They pay a service fee to the host company.

Windows 10 and 11 extensively use cloud computing with One Drive.

A disadvantage of Cloud computing is if the Internet is down you can't access your applications and data.

Review Questions:

1. Where would you use a Domain user account?

_____

_____

_____

2. What does NetBIOS stand for and what does it do.

_____

_____

_____

3. What is one purpose of a redirector program?

_____

_____

_____

4. What protocol would you use to access the internet?

_____

5. On what type of network would you use a Workgroup or Homegroup?

_____

Not to be reproduced without permission

6. Describe four differences between a Peer to Peer network and a Server based network.

7. What is the role of a network Administrator.

8. What are 3 advantages or a Peer to Peer network over a Client/Server network?

9. What are 3 advantages of a Client/Server network over a Peer to Peer network?

10. What is the main advantage of putting Users in Group accounts?

11. What is one advantage of Cloud computing?

Not to be reproduced without permission

Skill Practice 4A

Introduction to Server Based Networks

Task

To provide an introduction to the user utilities on a Windows server based Lan.

Equipment

- Functional computer with Windows installed.
- Network + guide to networks demo disk with Test Out program.
- Speakers for PC.

Procedure

Using simulation software.

1. Boot the computer to Windows and run the Testout program from programs menu. You will need to have the Testout CD in CD-ROM. If Testout is not installed on your PC, install by running setup and follow the prompts.

2. When you run Testout it will ask for a logon ID. Enter your initials, then click LOGON. In the auto register box enter your first name. Click OK.

3. At the next screen click start.

4. Select **4.0 Basic Windows 2000 networking tasks.**

5. Select **4.3** Windows 2000 client and service software tasks.

6. Run the **Demo 4.3.1.** (Double click) **Installing and working with client software.**

7. Run the **Lab 4.3.2.** (Double click) This will run a simulated program that represents a Windows 2000 computer. Follow the scenario, when finished click done. If

Not to be reproduced without permission

successful you will have a tick, if not go to explanation and it will tell you the correct procedure.

8. Run Lab 4.3.3
9. Run Lab 4.3.4
10. Run Demo 4.3.5 Using and mapping drives to shared folders.
11. Run Lab 4.3.6
12. Run Lab 4.3.7
13. Run Demo 4.3.13 Sharing folders using Windows explorer.
14. Run Demo 4.3.14 Sharing folders using Windows management.
15. Run Lab 4.3.15
16. Run Demo 4.3.18 Creating and working with Local User accounts.
17. Run Lab 4.3.19
18. Run Demo 4.3.16 Sharing Printers
19. Run 4.3.17 Sharing Printers
20. Run Demo 4.3.22 Configuring permissions for folders.
21. Run Demo 4.3.23 Configuring permissions for printers
22. Run Lab 4.3.24

End of practical exercise.

Student Notes:

Section 5

LAN Installation & Planning

Purpose

To understand the importance of correct planning of a LAN

Objectives

At the end of this section you should be able to:

- Understand the reasons why we need to plan a LAN.
- Network interface cards NIC's
- Design a client server LAN both Logical and Physical.
- Identify hardware requirements
- Understand print servers
- Document a LAN

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 17 & 18

Not to be reproduced without permission

Planning and Installing a Local Area Network

The 4 Steps to planning a LAN

There are 4 steps to planning a LAN

1. Design

   Both Logical and Physical

2. Implementation
3. Operations and Maintenance
4. Documentation

Each of these steps will be discussed in further detail and broken down into smaller steps.

Design

Before you can design a LAN you have to do some initial planning. Most of this initial planning is done with consultation with your customer. To plan a LAN you must first of all have a clear statement of the LAN's goals and objectives. You must also have an understanding of how the business actually functions on both on both administrative and physical aspects. The following issues should be addressed. What functions of the business need to be supported by the LAN?

- What administrative functions need to be supported?
- What improvements are being sought by implementing a LAN?
- What is the main purpose of the LAN?

Planning also involves looking a current infrastructure that is already in use.

- What work stations are currently in use?
- What Operating system are they using?
- Will these PC be attached to the new LAN?
- What software is currently being used? Will it be continued to be used? Do they have site licenses?
- Does their network connect to a WAN?
- Which computer acts as the print server
- What level of skills do the users have? Are they capable of using a new LAN or do they need training.
- How much money do they want to spend?

Not to be reproduced without permission

Software considerations

When assessing the network operating system software and client software, consider the following:

- What types of protocols are needed? TCP/IP, IPX/SPX, AppleTalk, SMB etc
- What kind of topology is being used?
- Will all the workstations need to access the internet?
- What level of security is required?

Hardware considerations

When deciding in the types of hardware required include the following:

- What type of network will it be Peer to Peer or Client / Server?
- What types of server will be required?

  File server

  Print server

  Communications server (Mail/Web)

- How powerful do the workstations need to be?
- What devices need to be shared, printers, backup devices, modems
- What type of connectivity devices will be needed? Hubs, Routers, Switches etc. Are they compatible with each other?
- What type of cabling will be needed?
- What speed is required on the network?
- Does the LAN need to be scalable (Will it need to expand)?
- Will it cope with large amounts of traffic?
- Does the application software require any special hardware requirements?
- Is the new hardware compatible with the current hardware and operating system?
- Are there NIC's to be installed in existing PC's or do they need to be upgraded to improve speed?

Implementation

The implementation of a LAN is a big consideration and needs to be coordinated with the customer. If an entirely new LAN is being installed the old system will need to be left in place until the new one is operational. Remember, employee's will still need to work. You need to implement the LAN with as little disruptions to the running of the business as possible. This may involve installing new equipment and software in stages.

Not to be reproduced without permission

The training of operators/users needs to be coordinated with the implementation of new equipment. No point having new equipment if you don't know how to use it.

A time line should be established with start and finish dates, showing when different areas of the network will be completed.

Operations and Maintenance

Once you have completed installing particular area of your LAN you need to ensure that they work and that you are on the right path. A way of accomplishing this is to test and evaluate your processes before moving on to the next. Once each task is implemented the whole network should be tested and verified that all aspects are working correctly.

All networks will require some sort of maintenance at some time. This may just be adding a new workstation or user. It could be upgrading hardware or software.

A plan must be included with your proposal as to who is responsible for these changes. You may provide a service contract that includes this type of work or you may charge it out on a per call basis. Often telephone support can be included.

Documentation

Keeping of accurate records can make upgrade or repairing a LAN a simple process.

Benefits of Network Documentation

Faster troubleshooting

Good documentation reduces the need to research solutions to the same problem each time the problem arises.

A visual diagram can help identify potential problem areas in a more timely manner.

Reduced information loss

Helps prevents loss of important network information when employees leave the organization, making the transition period less painful.

Easier task sharing

Network administrators can successfully delegate network responsibilities because important information is available in written form.

Improved network design

A current network diagram is a key element in any design process.

Not to be reproduced without permission

Software Upgrades

If the customer was going to install a new software program that has certain hardware requirements, it is a lot easier to look up a document than have to go to every machine on the network to see its capabilities.

What is the GREATEST benefit to you?

Complete up-to-date network documentation will save you TIME!

How much information do I need to include?

Theoretically

A good rule of thumb is to include everything you would need to rebuild your ENTIRE network from scratch.

Realistically

The amount and depth of your documentation will vary depending on the complexity of your network and the resources you have to create/collect the documentation.

Examples of information you might include are:

Building diagram/floor plan

Physical network diagram

Logical network diagram

Hardware information

Configuration information

Protocol information

DNS information

Network administration information

- Contact information
- Vendor information
- Device log sheets
- Procedure documentation
- Acceptable use policy
- Security policy
- Disaster recovery plan
- Software documentation

Not to be reproduced without permission

Network Interface Cards (NIC)

Network Adapter Software

You must ensure that no matter what your operating system, whether it is Windows 7, Win 8, Win 10, Win 11, Linux or any other OS, that the correct device driver is installed for the network adapter and that it is configured correctly.

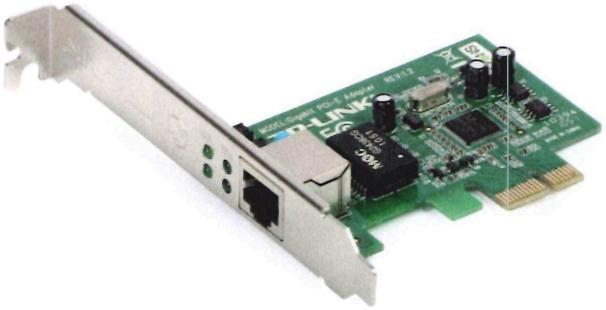
A device driver is software that enables the device to communicate with the computer's operating system. When you add hardware, you must install the device drivers. Some operating systems, such as Windows, come with a multitude of built-in device drivers. In that case, after you physically install new hardware and reboot, the operating system will automatically recognise the hardware and install the device's drivers. Each time a computer boots up, the device drivers for all its connected peripherals are loaded into RAM so that the computer can communicate with those devices at any time.

If operating system does not contain appropriate device drivers for the network card you have added, you need to load the suitable driver supplied with the NIC. If you don't have the correct driver you will need to download it from the manufactures web site. On some occasions if your network card stops working you can reset your network, and Windows will automatically install the correct driver.

Most motherboards come with a NIC built into them, so it is rare that you need to install a network card. You still sometimes need to install wireless network card on a desktop computer to enable you to connect to a wireless network.

Physical network address

Each NIC has a physical address called the **MAC address**. (Medium Access Control). The MAC address is stored in ROM in the network card and is unique to each card. Each manufacturer uses a different identifying number so no two cards will have the same number.



Pic: PCI- Express Network Interface Card

Review Questions:

1. Name three benefits of effective communication with customer prior to planning a LAN.

_____

_____

_____

2. Which of the following implementation steps should come first?

   a. Find vendors for necessary hardware additions

   b. Determine the cost of the proposed project

   c. Evaluate how users' needs might conflict with implementation

   d. Identify the needs of the LAN

3. What is the last step in a network implementation project?

_____

4. Time lining will help you determine how long a project should take.

   True or False?

5. Give three examples of why you would want security on your network.

_____

_____

_____

6. What are five benefits of documenting your LAN?

_____

_____

_____

_____

_____

Not to be reproduced without permission

7. Why is it important to test and evaluate you LAN during implementation?

_____

_____

_____

_____

Additional Notes:

Not to be reproduced without permission

Skill Practice 5A

Planning a LAN

Task

To work in small groups of 3 or 4 students, plan a Local Area Network, as described below. At completion of the task a group member will present your groups outcomes to the class for a brief discussion.

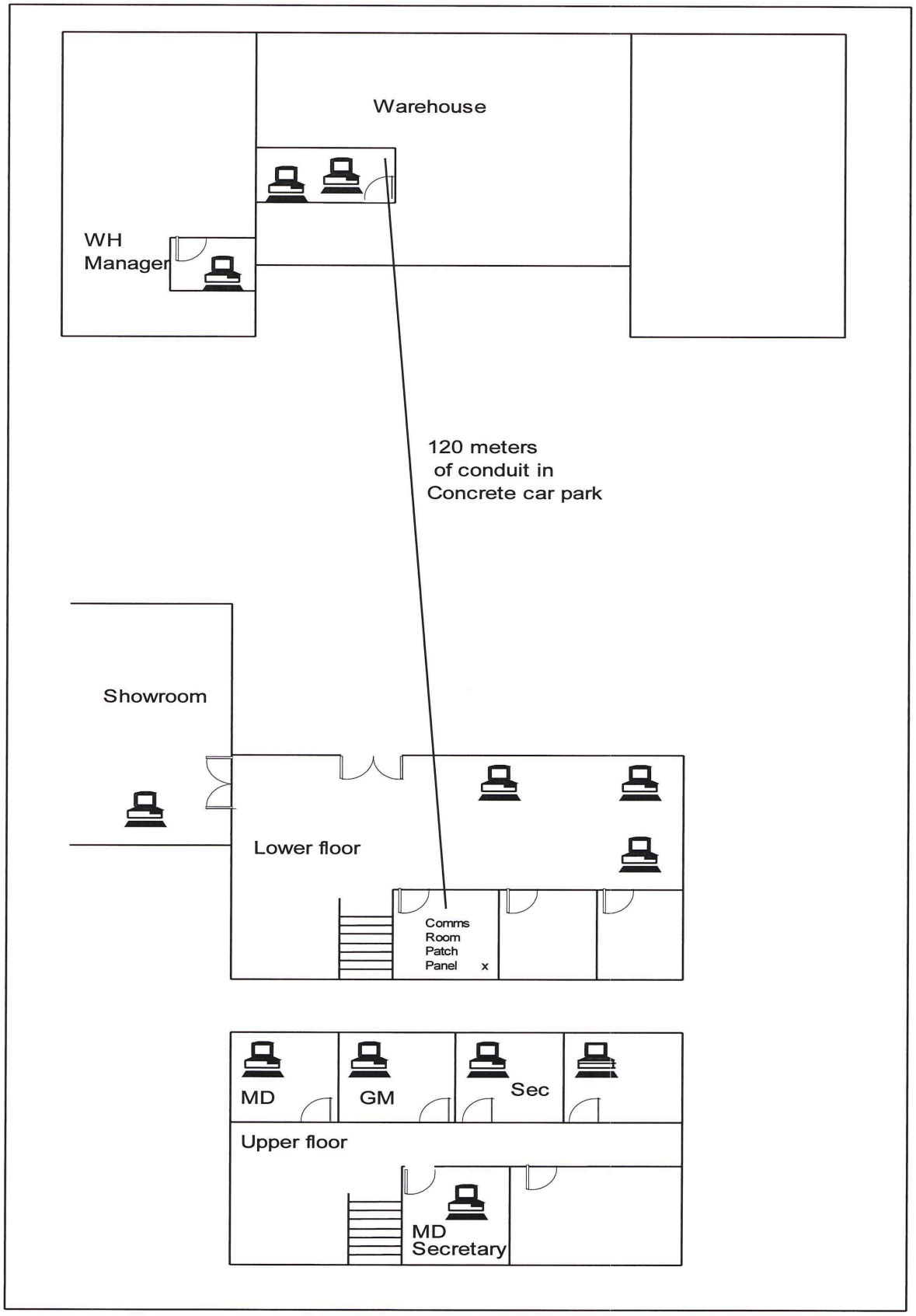
Case project

You have been asked to plan a LAN at a Manufacturing / Retail business located on the Central Coast. The Administration office is a 2-storey building that will have 5 PC's located upstairs, 2 for the managers, 2 for their secretary's and an Apple Mac for their desktop publishing. The MD's secretary is responsible for system administration and backups. A laser printer is located in each of the secretary's offices. Downstairs there will be 3 PC's in the office area. There is one digital copier connected using TCP/IP as a printer and scanner. There will also be a colour inkjet printer connected to a PC. There is another PC located in the showroom with a docket printer attached. In the rear of the lower office is a communications room that contains a patch panel.

The warehouse is located 120 meters away where there will be 3 PC's. 2 in dispatch and one in the warehouse managers office. Each PC has its own dot matrix printer attached.

All workstations will be using Windows 11 professional and connected to a file server running Windows 2022 server. Each PC will have MS Office 2019 and Xero accounting software (Network version). Each user will have restricted access to programs and documents. The manager is paranoid about data loss and unwanted intrusion on his network. The business has retail stores throughout the state.

Not to be reproduced without permission



Not to be reproduced without permission

Procedure

Discuss in groups and decide what equipment needs to be included in LAN eg: Cable, hub's, Routers, PC's, Printers, UPS's etc.

Decide on the most suitable location of file server, hubs, printers etc.

Should the system be Peer to Peer or client/server. Why. What topology should be used.

Include any other equipment that might be beneficial to support and operate LAN. The customer does not want to use wireless technology because of lack of security. Which computer will act as the print server for the digital/copier/printer/scanner?

Have a spokesperson from your group present findings to class.

Not to be reproduced without permission

Not to be reproduced without permission

Section 6 LAN Interconnectivity

Purpose

To understand the different types of network connectivity devices and know their uses. Know and understand TCP/IP protocol.

Objectives

At the end of this section, you should be able to:

Explain the purpose and operation of:-

- Hubs
- Switches
- Repeaters
- Routers
- Bridges
- WAN
- TCP/IP Protocol
- UDP
- IP Addressing

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 18

Not to be reproduced without permission

Hubs and Repeaters

A simple hub is a multiport repeater. A hub has a number of outlets on it which are known as ports. Hubs come in numerous types and sizes and are referred to by the number of ports that they have. Common size hubs are 4, 5, 8, 10, 16, or 24 ports. Some will come with an uplink port for connecting multiple hubs together. Hubs are used to join multiple computers or other network devices together to form a single network segment. Ethernet hubs are the most common.

A hub operates in layer 1 of the OSI model. Hubs do not read any of the data passing through them and are not aware of packet source or destination. A hub essentially receives incoming packets and broadcasts these packets out to **all** devices on the network.

Most cheaper hubs are passive and do not alter the signal. An active hub will regenerate the incoming signal to remove attenuation. (losses)

You can have a maximum of 4 hubs / repeaters, which will make 5 segments.

Hubs have disappeared in networking and a switch is used instead.

Bridges and switches

1. A bridge is a device that looks like a repeater. It has 2 ports, an input and an output port. A bridge has the ability to examine data frames and know the correct destination to forward them to. The bridge reads the destination MAC address and decides whether to forward the frame to another segment or whether it belongs to the source segment. This is done by a Forwarding Table that is created by the bridge. This is a database of all known MAC addresses and location on the network. The bridge uses this database to know whether to forward or filter the packets. In this way a Bridge can ensure that areas of high data traffic on a Ethernet LAN can be separated into segments, leaving other segments to carry there own traffic.

2. As Bridges cannot interpret higher level protocols such as TCP/IP, AppleTalk, SPX/IPX and NetBIOS, they also have the ability to connect different types of LANs together such as Ethernet and devices used by IoT (Internet of Things). The Bridge will perform additional functions of protocol conversion.

3. One problem which occurred with early Bridges is that of loops in a network which allow more than one way of reaching a destination. If a loop was detected all traffic would be forwarded. In order to prevent the problems a Spanning Tree Algorithm is used, this is a routine that can detect circular traffic patterns and modify the way multiple bridges work together in order to avoid these patterns. The specifications for the Spanning Tree Algorithm are found in IEEE 802.1d. Bridges operate in the data link layer (Layer 2) of the OSI model.

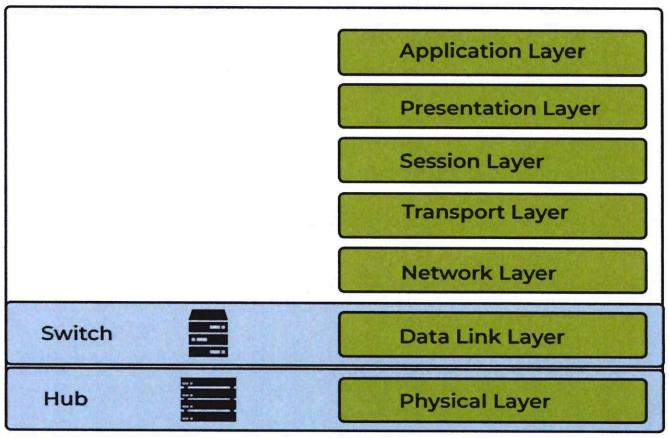
Not to be reproduced without permission

Switches

A switch a multiport bridge and is a hub that is taken to the next level. To look at they appear the same.

A switch has the ability to filter and send data to specific hardware ports. If a packet comes into a switch, it can choose the correct path rather than broadcasting to the entire network. This can help eliminate network congestion.

Switches often have advanced filter options, bandwidth metering, and traffic statistics. A switch is a multi port bridge. Switches operate in Layer 2.



Pic: OSI layers

Types of switches. (To name a few)

Managed switched

Managed switches, most seen in commercial and enterprise settings, provide greater capacity and capabilities for IT experts. To configure managed switches, command-line interfaces are utilized. They enable simple network management protocol agents, which offer information for troubleshooting network issues.

Unmanaged switches

The most basic switches are unmanaged switches, which have a set configuration. An unmanaged switch merely expands a LAN's Ethernet connections, allowing additional internet connections to local devices. Unmanaged switches use device MAC addresses to transmit data back and forth. They are usually plug-and-play, meaning the user has few alternatives to pick from.

Power over Ethernet (POE) switches

PoE capabilities are now available on some network switches, making installing IoT devices and other gear faster, simpler, and safer. PoE is a method of supplying DC

Not to be reproduced without permission

power to low-power devices across a LAN wire. Low-power devices connected to a PoE-capable network switch will no longer require a power supply. When concealing connections isn't possible, this avoids the need for additional power outlets and makes the installation seem efficient. A PoE-capable switch is also safer because the power output is low and intelligently managed.

PoE Standards and Wire Usage

IEEE 802.3af / 802.3at (PoE / PoE+)

- **Mode A (Endspan):** Power is delivered over the *data pairs* (pins 1, 2, 3, and 6).
- **Mode B (Midspan):** Power is delivered over the *spare pairs* (pins 4, 5, 7, and 8).
- Devices must support both modes to be fully compliant.

IEEE 802.3bt (PoE++ / 4PPoE)

- **Type 3 and Type 4:** Power is delivered over *all four pairs* (pins 1–8).
- Enables higher power delivery (up to 60W for Type 3, and up to 100W for Type 4).

Stackable switches

Stackable switches allow you to optimize your network while also increasing its reliability. With an actual stackable switch, these clusters of switches function as a single switch powered by a single SNMP/RMON agent, one domain, just one command line interface (CLI), or a Web interface.

Layer 3 switches

Switches are part of the OSI model's Layer 2 layer. They function at the data network layer, and their main job is to forward ethernet frames as quickly as possible from one port to another. Because they operate at the Network Layer of the OSI model, these switches are referred to as Layer 3 switches. A Layer 3 switch is a hybrid of Layer 2 and 3 devices. Their software is more complex than traditional Layer 2 switches, and they can run dynamic routing protocols.

Layer 4 switches

Layer 4 switches are commonly used in:

- **Data centre's** to balance web traffic across server farms
- **Enterprise networks** to enforce application-specific policies
- **VoIP and video streaming** to ensure low latency and jitter
- **Security appliances** for advanced traffic filtering

Layer 4 switches are beyond the scope of this unit.

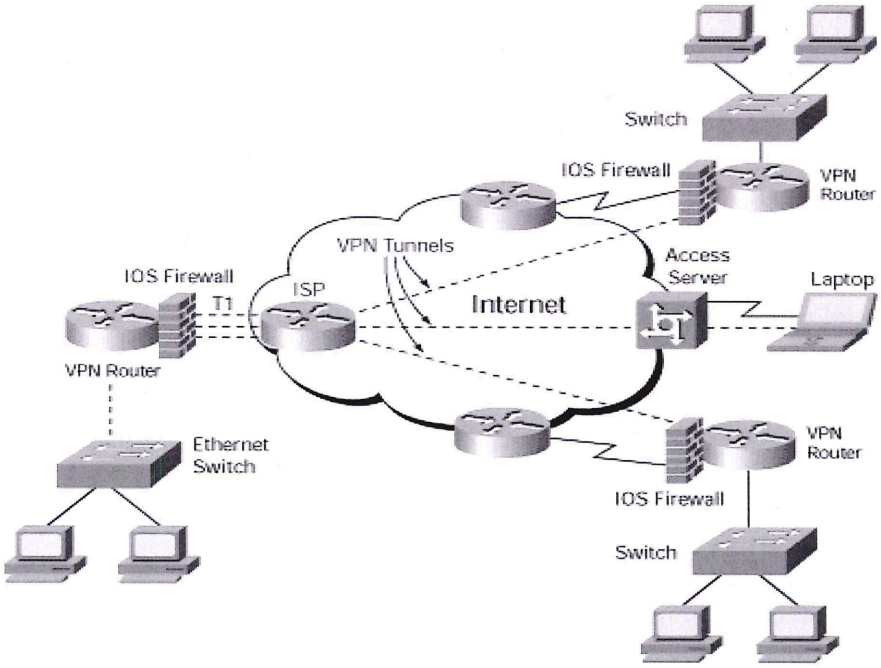


Figure 6-1 A typical LAN connecting to a WAN

Routers

A router is your core LAN hub and it manages data flow to and from your end devices. Modern routers also have built-in modems, which means that they can receive connectivity signals from the external network and relay it to end devices from a singular appliance.

A router is a multiport connectivity device that can integrate LANs and WANs, running at different speeds and using different protocols. Routers operate in layer 3 of the OSI model (Network). A router will communicate with other routers and produce an internal routing table that reflects the whole network. This routing table enables the router to find the shortest possible path between nodes. The routing table is updated every 30 seconds. A Router can also connect dissimilar network together. The internet relies on a multitude of routers throughout the world. Routers also enable all users on a LAN to share a single connection to the Internet or WAN.

Routing protocols

Routing protocols are used to determine the best path through the network. A routing protocol is different to a routable protocol such as TCP/IP or IPX/SPX. Routing protocols are used to collect data about the current network status and contribute to select the best paths to be taken.

There are 4 common routing protocols

RIP Routing Information Protocol for IP and IPX

OSPF Open Shortest Path First for IP

EIGRP Enhanced Interior Gateway Routing Protocol for IP IPX and AppleTalk.

BGP Border Gateway Protocol - used for Internet backbones

Access points

Access points and routers are located within the LAN environment.

Access points are a staple of enterprise LAN architecture. They let you extend the wireless coverage of your local area network so that you can group hundreds or thousands of end devices spread across a massive office campus into a single LAN.

WAN - Wide Area Networks

Often a network is located in multiple physical locations. Wide area networking is the connecting of multiple LAN's that are geographically isolated. This is achieved by the use of dedicated leased telephone lines, dial up telephone lines, broadband telephone lines , broadband cable or satellite links.

A WAN can be as simple as providing modems and a remote access server to allow employees to dial in, or it could be as complex as linking 100's of branch offices across the world using special WAN protocols.

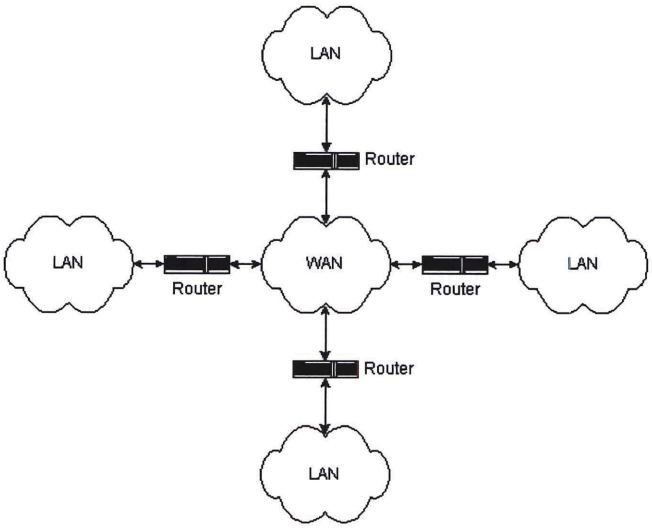


Figure 6-2 4 LAN's connect as WAN

TCP/IP

TCP and IP were developed by a Department of Defense research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet. On the battlefield a communications network will sustain damage, so the DOD designed TCP/IP to be robust and automatically recover from any node or phone line failure. This design allows the construction of very large networks with less central management. However, because of the automatic recovery, network problems can go undiagnosed and uncorrected for long periods of time.

As with all other communications protocol, TCP/IP is composed of layers:

TCP Is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

IP Is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world.

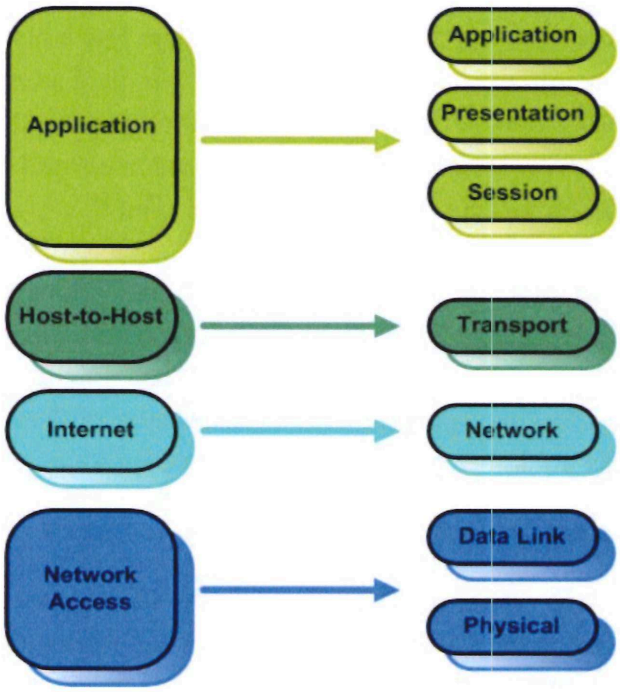
Sockets - is a name given to the package of subroutines that provide access to TCP/IP on most systems.

TCP/IP and the OSI Model Comparison

If we compare TCP/IP and the OSI Models we can see the TCP/IP model is basically a shorter version of the OSI model. It consists of four instead of seven layers. Despite their architectural differences, both models have interchangeable transport and network layers and their operation is based upon packet-switched technology. The diagram below indicates the differences between the two models:

Not to be reproduced without permission

The TCP/IP and OSI Models



Application Layer: The Application layer deals with representation, encoding and dialog control issues. All these issues are combined together and form a single layer in the TCP/IP model whereas three distinctive layers are defined in the OSI model.

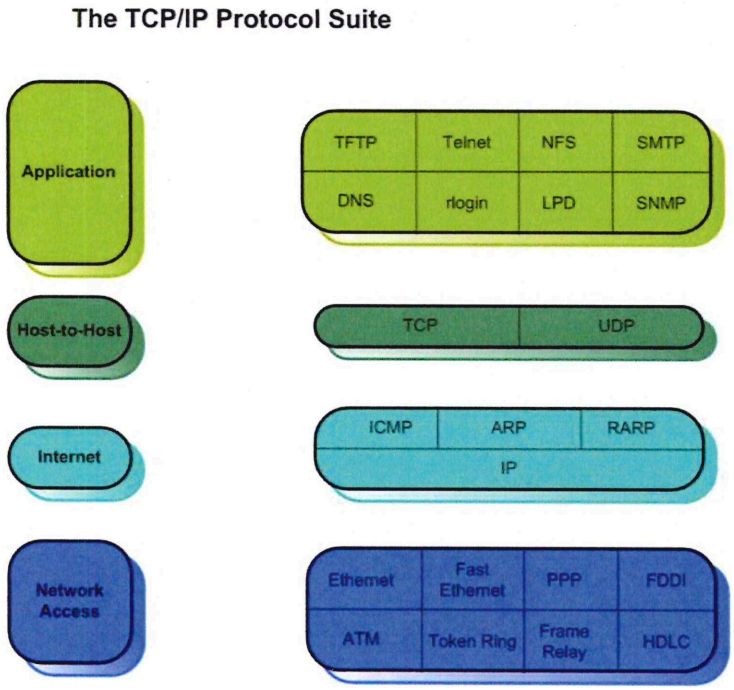
Host-to-Host: Host-to-Host protocol in the TCP/IP model provides more or less the same services with its equivalent Transport protocol in the OSI model. Its responsibilities include application data segmentation, transmission reliability, flow and error control.

Internet: Again, Internet layer in TCP/IP model provides the same services as the OSIs Network layer. Their purpose is to route packets to their destination independent of the path taken.

Network Access: The network access layer deals with all the physical issues concerning data termination on network media. It includes all the concepts of the data link and physical layers of the OSI model for both LAN and WAN media.

Not to be reproduced without permission

The diagram below shows clearly the way TCP/IP protocol suite relates to the TCP/IP model.



Host-to-Host Layer Protocols

Two protocols: **Transmission Control Protocol** (TCP) and **User Datagram Protocol** (UDP) are defined for transmitting datagrams. We will look at the details of both these protocols as well as their interaction with the upper layer.

Transmission Control Protocol (TCP)

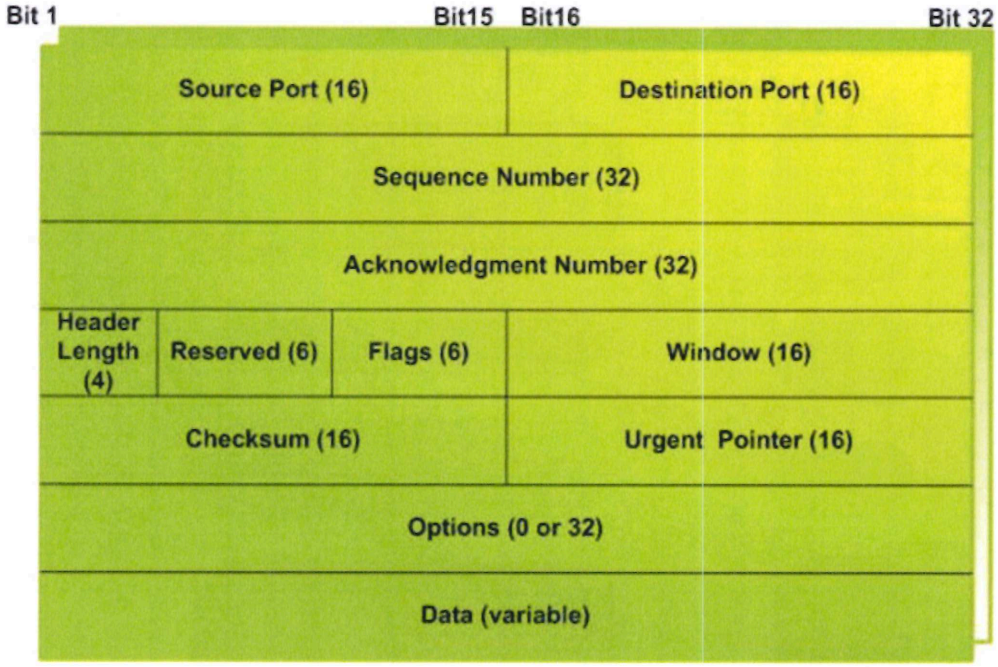
TCP is connection-oriented in the sense that prior to transmission end points needs to establish a connection first. TCP protocol data units are called segments. The sending and receiving TCP entities exchange data in the form of segments, which consist of a fixed 20-byte header followed by a variable size data field.

TCP is responsible for breaking down a stream of bytes into segments and reconnecting them at the other end, retransmitting whatever might be lost and also organizing the segments in the correct order. The segment size is restricted by the maximum transfer unit (MTU) of the underlying link layer technology (MTU is generally 1500 bytes which is the maximum payload size of the Ethernet).

The image below shows the TCP segment format. The most important fields are explained further on.

Not to be reproduced without permission

The TCP Segment Format



- **Source Port** and **Destination Port** fields together identify the two local end points of the particular connection. A port plus its hosts' IP address forms a unique end point. Ports are used to communicate with the upper layer and distinguish different application sessions on the host.
- The **Sequence Number** and **Acknowledgment Number** fields specify bytes in the byte stream. The sequence number is used for segment differentiation and is useful for reordering or retransmitting lost segments. The Acknowledgment number is set to the next segment expected.
- Data offset or **TCP header length** indicates how many 4-byte words are contained in the TCP header.
- The **Window** field indicates how many bytes can be transmitted before an acknowledgment is received.
- The **Checksum** field is used to provide extra reliability and security to the TCP segment.
- The actual **user data** are included after the end of the header.

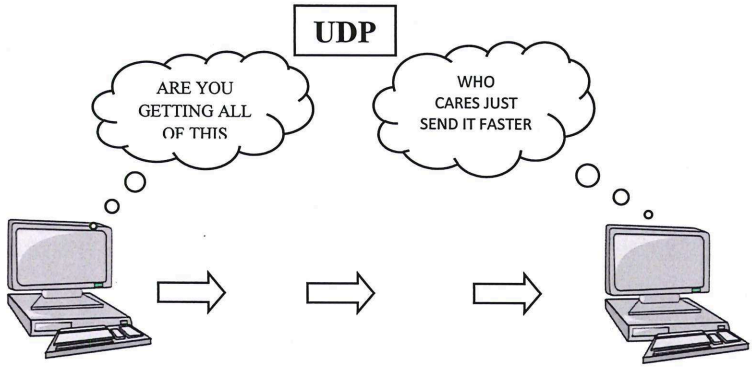
User Datagram Protocol (UDP)

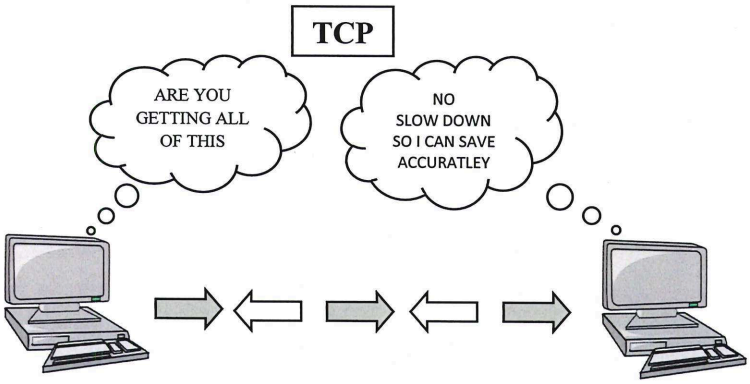
UDP (User Datagram Protocol) is another commonly used protocol on the Internet. However, UDP is never used to send important data such as webpages, database information, etc; UDP is commonly used for streaming audio and video. Streaming media such as Windows Media audio files (.WMA) , Real Player (.RM), and others use UDP because it offers speed! The reason UDP is faster than TCP is because there is no form of flow control or error correction. The data sent over the Internet is

affected by collisions, and errors will be present. UDP is **only** concerned with speed. This is the main reason why streaming media is not high quality.

UDP protocol consists of fewer fields compared to TCP. The reason for that is because certain data types do not require reliable delivery and extra overhead. Real-time traffic for example, needs to be transported in an efficient way without error correction and retransmission mechanisms.

UDP is considered to be a connectionless protocol. It leaves reliability to be handled by the application layer. All it cares about is fast transmission.





UDP Packet structure

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP

Not to be reproduced without permission

does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

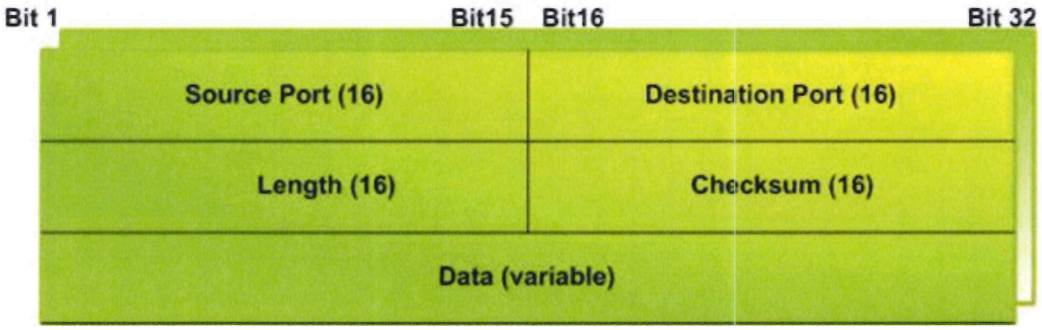
UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

UDP is a minimal message-oriented Transport Layer protocol. (layer 4, like TCP)

UDP provides no guarantees to the upper layer protocol for message delivery and the UDP protocol layer retains no state of UDP messages once sent. For this reason, UDP is sometimes referred to as *Unreliable* Datagram Protocol.

UDP provides application multiplexing (via port numbers) and integrity verification (via checksum) of the header and payload. If transmission reliability is desired, it must be implemented in the user's application. The UDP header consists of 4 fields, each of which is 2 bytes (16 bits). The use of the fields "Checksum" and "Source port" is optional in IPv4. In IPv6 only the source port is optional.

The UDP Segment Format



Source port number

This field identifies the sender's port when meaningful and should be assumed to be the port to reply to if needed. If not used, then it should be zero. If the source host is the client, the port number is likely to be an ephemeral (short lived) port number. If the source host is the server, the port number is likely to be a well-known port number.

Destination port number

This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be a short-lived port number and if the destination host is the server then the port number will likely be a well-known port number.

Length

A field that specifies the length in bytes of the entire datagram: header and data. The minimum length is 8 bytes since that's the length of the header. The field size sets a theoretical limit of 65,535 bytes (8 byte header + 65,527 bytes of data) for a UDP datagram. The practical limit for the data length which is imposed by the underlying IPv4 protocol is 65,507 bytes (65,535 – 8 byte UDP header – 20 byte IP header).

In IPv6 Jumbograms it is possible to have UDP packets of size greater than 65,535 bytes. This allows for a maximum length value of 4,294,967,295 bytes (2^32 - 1) with 8 bytes representing the header and 4,294,967,287 bytes for data.

Checksum

The checksum field is used for error-checking of the header *and* data. If no checksum is generated by the transmitter, the field uses the value all-zeros. This field is not optional for IPv6.

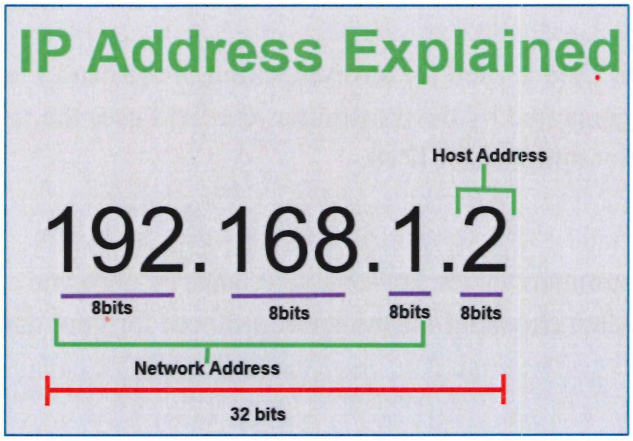
The following table summarizes the key-characteristics of each one of these protocols. Keep them in mind when choosing the transport protocol for your data.

Not to be reproduced without permission

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Pic: TCP V's UDP

IP addressing (IPv4)



An IP address is 32 bits wide, and it is composed of two parts: the network number, and the host number. The network portion is common to all nodes on the network, whereas the host portion is unique to each device. By convention, it is expressed as four decimal numbers separated by periods, such as "203.138.32.3" representing the decimal value of each of the four bytes. Valid addresses thus range from 0.0.0.0 to 255.255.255.255, a total of about 4.3 billion addresses. The first few bits of the address indicate the Class that the address belongs to:

The bits are labeled in network order, so that the first bit is bit 0 and the last is bit 31, reading from left to right. Class D addresses are multicast, and Class E are reserved. The range of network numbers and host numbers may then be derived:

Class Range of Net Numbers Range of Host Numbers

Class	Description
Class A	Have network addresses from 1.0.0.0 through 127.0.0.0. The network number is the first octet, being from 1 to 127. That number uniquely identifies the class A destination network. The rest of the address, 3 octets, uniquely identifies a machine within that network.
Class B	Have network addresses from 128.0.0.0 through 191.255.0.0. The network number is the first two octets, being from 128.0 to 191.255. This number uniquely identifies the class B destination network. The rest of the address, 2 octets, uniquely identifies a machine within that network.
Class C	Have addresses from 192.0.0.0 through 223.255.255.0. The network number is the first three octets, being from 192.0.0 through 223.255.255. Each class C network can have one octet worth of hosts.
Class D	Have addresses from 224.0.0.0 to 239.255.255.255. Class D network addresses are used for multicast protocols. Multicasting allows one device to send to a specific group of devices not the entire network segment.
Class E	Have addresses from 240.0.0.0 to 255.255.255.255. Class E networks are reserved for future use.

Number of networks and hosts per network class.

Network Class	Beginning Octet	Number of Networks	Hosts per Network
A	**1-126**	**126**	**16777214**
B	**128-191**	**>16,000**	**65534**
C	**192-223**	**>2,000,000**	**254**

Not to be reproduced without permission

127.xxx.xxx.xxx

Any address starting with 127 is a loop back address and should never be used for addressing outside the host. The loop back address is used for testing purposes.

Most users connected to the Internet will be assigned addresses within Class C, as space is becoming very limited. This is the primary reason for the development of IPv6, which will have 128 bits of address space.

DHCP

DHCP stands for Dynamic Host Configuration Protocol and provides a solution that automatically assigns IP addresses to computers on a network. When a client is configured to receive an IP address automatically, it will send out a broadcast to the DHCP server requesting an address. The server will then issue a "lease" and assign it to that client. The time period that a lease will last can be specified on the server. Some of the benefits of DHCP include the following:

- Prevents users from making up their own IP addresses.
- Prevents incorrect gateway or subnet masks from being entered by your help desk.
- Decreases amount of time spent configuring computers especially in environments where computers get moved around all the time.
- Handy in situations where you have a large sales staff that only have to work 1 day a week. On that one day they bring their laptops and they can just plug them into the network and they are all set.
- Overcomes the problem of a company who has 300 workstations and only 254 assignable IP address.
- DHCP uses host names (eg: full computer name).

If the lease expires and the client is unable to get a new one then the user will not be able to communicate over the network.

Subnet Masks

Your computer has no way of knowing what kind of IP address you have, this means that there has to be some way of letting your software extract the network ID from the IP address. To do this, you can use subnet masks. Typically a subnet mask will look like this: 255.255.255.0. This tells us quickly that we are using a Class C IP address as the first three 255's tell us that these individual numbers can't change. The zero tells us that this is the only digit that we can use, so it has to be a Class C IP address.

If we had an IP address of 128.10.11.23 and a subnet mask of 255.255.0.0 then we can quickly see that we have a Class B IP address. The whole point of a subnet mask is to tell the computer which is the Network ID and which is the host ID.

Not to be reproduced without permission

Private IP Address

As well as the reserved IP addresses, there are other addresses which are not used for the internet and are used for private networks.

The following IP addresses are allocated for private networks.

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

169.254.0.0 to 169.254.255.255

The 10 network is usually used for larger networks. The 172 network is used for smaller companies and broken up into smaller subnets. Most home users and small office networks use the 192 network.

The 169 network is used when DHCP is not available.

IPv6

IPv6 is the newest version of internet protocol formulated by the Internet Engineering Task Force (IETF), which helps identify and local endpoint systems on a computer network and route online traffic while addressing the problem of IPv4 address depletion due to prolonged internet use worldwide.

Internet protocol version 6 (IPv6) is a network layer protocol that allows communication to take place over the network. Each device on the internet has a unique IP address used to identify it and figure out where it is. At the time of the digital revolution of the 1990s, it became apparent that the IP addresses that Internet Protocol version 4 (IPv4) used to connect devices would not be enough to meet demand.

The IETF set on developing the next-generation internet protocol. IPv6 became a draft standard for the IETF in December 1998, and on July 14, 2017, it was approved as an internet standard for global rollout.

Limitations of IPv4 and the need for IPv6

IPv4 addresses were getting depleted due to the rapid growth of internet users, high usage of devices such as mobiles, laptops, and computers, inefficient address use, and always-on devices like cable modems.

IPv6 has a 128-bit address and has a larger address space available for future allocation. The 128-bit address is broken into 8 groups, each containing 16 bits. Four hexadecimal numbers represent each group, and colons are used to divide each group from the others. IPv6 provides a host connected to the network with a unique identifier specific to the subnet.

Not to be reproduced without permission

Skill Practice 6B:

Mapping a Network Drive - Select version of windows you are using.

Windows 7

1. Double click on my network places and select tools from menu bar.
2. Select Map Network drive item.
3. In the Drive tab select a drive letter (use arrow to see vacant drive letters)
4. Select browse to view shared network folders. Select folder indicated by teacher. (This will be a workstation that is not being currently used by a student). Click OK after selecting drive.
5. Record the path that is shown in Folder box.

   _____

6. Make sure the reconnect at login box is ticked.
7. Click finish.
8. Go to My Computer. Can you see the network drive you just mapped?
9. Click on Network Drive to see if you can access contents.
10. Reboot into Windows. Can you still see mapped drive?
11. We will now remove the network drive. Right Click on the network drive you mapped. Click disconnect. Your mapped drive will disappear. Reboot PC to make sure it is gone.
12. Call teacher to check your work.

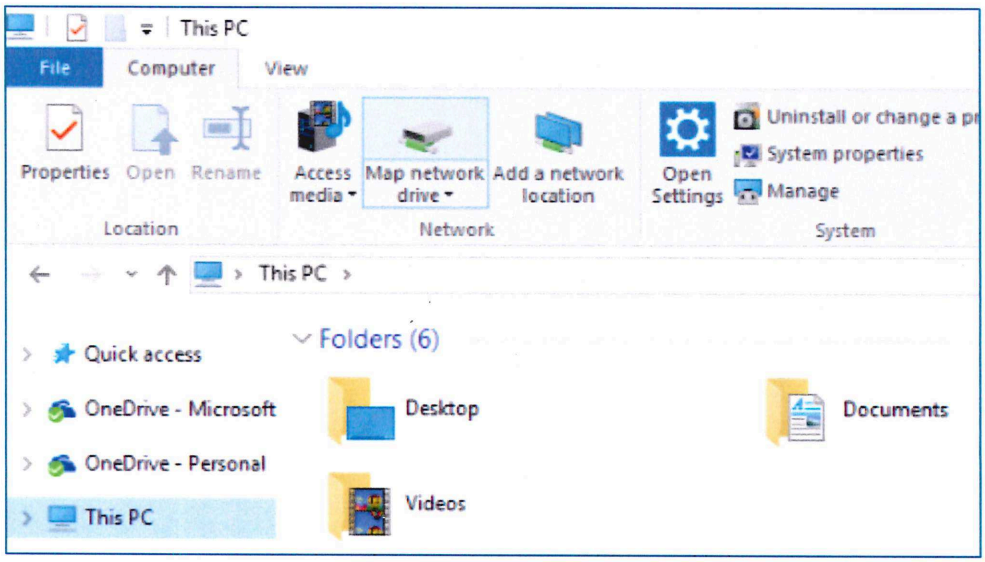
Not to be reproduced without permission

Map a drive in Windows 10

Map a network drive to get to it from File Explorer in Windows without having to look for it or type its network address each time.

1. Open **File Explorer** from the taskbar or the **Start** menu, or press the **Windows logo key** + **E**.

2. Select **This PC** from the left pane. Then, on the **Computer** tab, select **Map network drive**.



3. In the **Drive** list, select a drive letter. (Any available letter will do.)

4. In the **Folder** box, type the path of the folder or computer, or select **Browse** to find the folder or computer. To connect every time you sign in to your PC, select **Reconnect at sign-in**.

5. Select **Finish**.

Note: If you can't connect to a network drive or folder, the computer you're trying to connect to might be turned off, or you might not have the correct permissions. Try contacting your network administrator.

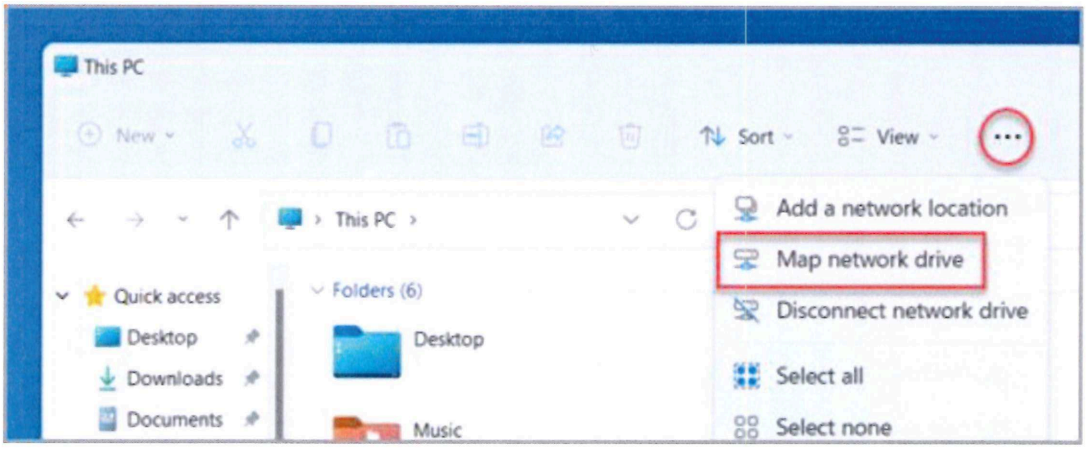
Not to be reproduced without permission

Map a drive in Windows 11

Map a network drive to get to it from File Explorer in Windows without having to look for it or type its network address each time.

1. Open **File Explorer** from the taskbar or the **Start** menu, or press the **Windows logo key** + **E**.

Select **This PC** from the left pane. Then, on the File Explorer ribbon, select **More** > **Map network drive**.



Note: If you don't see Map network drive on the More menu, you can right-click the **This PC** node in the folder pane and you'll see the command there.

2. In the **Drive** list, select a drive letter. (Any available letter will do.)
3. In the **Folder** box, type the path of the folder or computer, or select **Browse** to find the folder or computer. To connect every time you sign in to your PC, select **Reconnect at sign-in**.
4. Select **Finish**.

Note: If you can't connect to a network drive or folder, the computer you're trying to connect to might be turned off, or you might not have the correct permissions. Try contacting your network administrator.

End of skills practical

Not to be reproduced without permission

Section 7 LAN Troubleshooting

Purpose

To be able to understand trouble shooting procedures and have an understanding of LAN trouble shooting tools, both hardware and software. This section is intended to be a basic introduction to the topic only.

Objectives

At the end of this section you should be able to:

- Explain the procedure you would use to trouble shoot a LAN.
- List some of the tools used to trouble shoot LANs.
- List some software utilities that you would use to trouble shoot a LAN.
- Know the purpose and application of each type of test equipment.
- Demonstrate the ability to locate, isolate and rectify hardware and software problems in a LAN

Reading

The material for this Section is found within the Andrews reference book at the following locations:

- Chapter 18

Not to be reproduced without permission

Fundamental procedures for troubleshooting LANs Introduction

To solve problems in a networked computer environment you require a logical, step by step, systematic approach. By working with this type of procedure you will easily be able to locate and repair problems.

Steps for troubleshooting network problems are as follows:

1. Define the problem. Carefully gather facts and document what you learn from people or systems that alerted you to the problem and keep that documentation handy.

2. Identify the scope of the problem.

   - Is it effecting the whole network,
   - Are all users on the network experiencing the problem at all times?
   - Is the problem limited to a specific area of the network,

     - or a specific group of users
     - or to a particular period of time?

3. Establish if anything has been changed on the network. Recent hardware or software changes may be causing the symptoms.

4. Determine the most probable cause of the problem. This diagnosis may include the following information gathering techniques:

   - Which user noticed it first.
   - What where they doing when it failed
   - Are there any error messages
   - Has it happened before
   - Is it repeatable- can you recreate the problem
   - Is there a difference between this and the time before

5. The trouble shooter must know the hardware and software configuration of the network.

6. Verify the physical integrity of the network connections (check cable connections, NIC installations, and power to devices), starting at the affected nodes and moving outward toward the backbone.

7. Verify the logical integrity of the network connection (such as addressing, protocol bindings, software installations, etc).

Not to be reproduced without permission

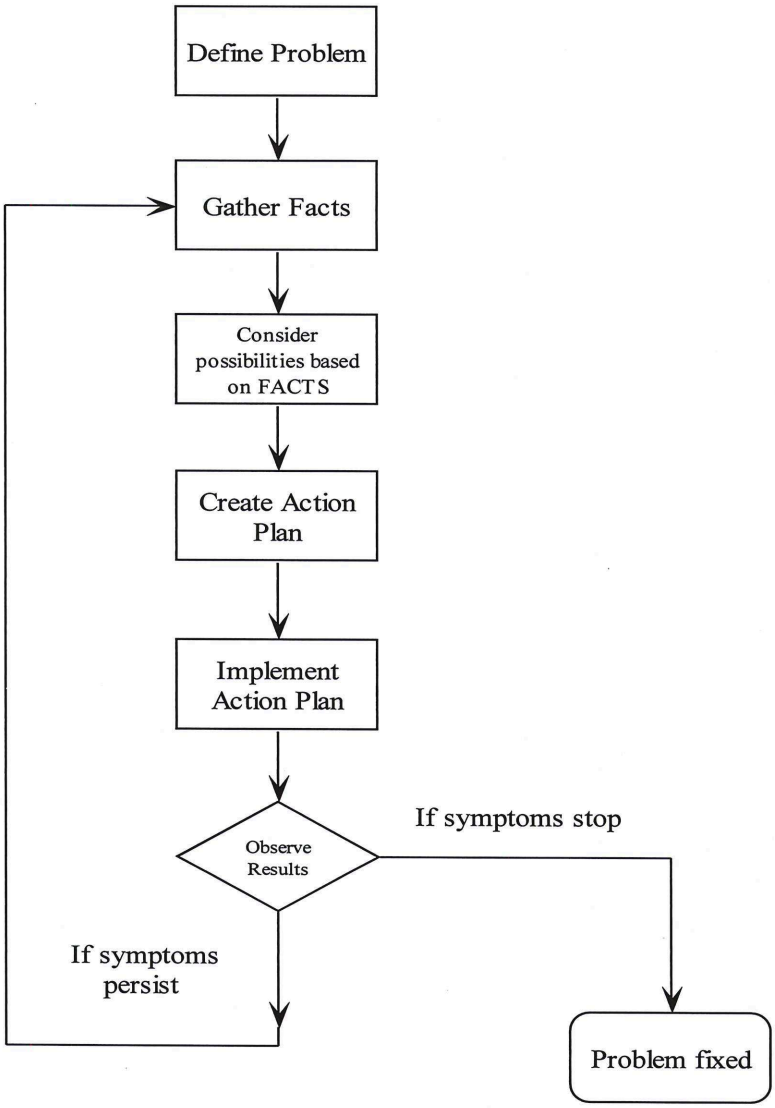
8. Implement a solution.

9. Test the solution.

10. Observe the results.

11. Document the solution. Make sure that both you and your colleagues understand the cause of the problem and how you solved it. This information should be kept in a centrally available repository, such as an online database.

A Simple flow chart for problem solving



Not to be reproduced without permission

TROUBLESHOOTING TOOLS

There are many tools designed to analyze and isolate network problems, ranging from simple cable testers that indicate whether a cable is faulty, to sophisticated protocol analyzers that capture and interpret all types of data traveling over the network.

The tool you choose will depend on the particular problem you need to investigate and the characteristics of your network.

The following sections describe a variety of network troubleshooting tools, their functions.

Hardware Troubleshooting Tools

Crossover Cable

A crossover cable is useful in troubleshooting to quickly and easily verify that a node's network adapter is transmitting and receiving signals properly. You can easily connect 2 workstations or a laptop together and test the ability for these 2 machines to communicate.

Multimeter

A **multimeter**, is a simple instrument that can measure many characteristics of an electric circuit, including its resistance and voltage. A multimeter is also used for testing continuity in cables

Cable Checkers

Basic **cable checkers** simply determine whether your cabling can provide connectivity.

To accomplish this task, they apply a small voltage to each conductor at one end of the cable, and then check whether that voltage is detectable at the other end. They may also check whether voltage cannot be detected on other conductors in the cable. Most cable checkers provide a series of lights that signal pass/fail.

As well as checking cable continuity, a good cable checker will verify that the wires are paired correctly and that they are not shorted, exposed, or crossed. Do not use a cable checker on a live network cable. Disconnect the cable from the network, and then test its continuity.

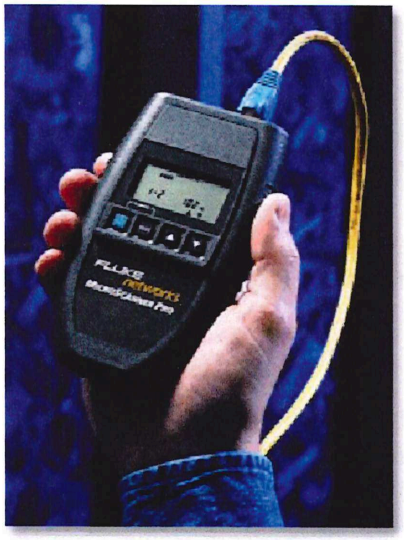
Cable Testers

The difference between cable checkers and cable testers lies in their sophistication and price. A **cable tester** performs the same continuity and fault tests as a cable checker, but also provides the following functions:

Not to be reproduced without permission

- Ensures that the cable is not too long
- Measures the distance to a cable fault
- Measures attenuation along a cable (Loss in signal strength)
- Measures near-end crosstalk between wires
- Measures termination resistance and impedance for Thinnet cabling
- Issues pass/fail ratings for CAT3, CAT5, CAT6, or even CAT7 standards
- Stores and prints cable testing results

Some cable testers may provide even more features, for example, a graphical output depicting a cable's attenuation and crosstalk characteristics over the length of the cable. Because of their sophistication, cable testers cost significantly more than cable checkers. A high-end unit may cost from $5000 to $8000, and a low-end unit may cost between $1000 and $4000. Popular cable tester manufacturers include Fluke and Microtest.



Picture 7-1 Fluke cable tester

Time Domain Reflectometers (TDRs)

1. A time domain reflectometer (TDR) is a high-end instrument for testing the qualities of a cable.

2. It works by issuing a signal on a cable and measuring the way the signal bounces back (or reflects) to the TDR. Connectors, crimps, bends, short circuits, cable mismatches, or other defects modify the signal's amplitude before it returns to the TDR, thus changing the way it reflects. The TDR then accepts and analyzes the return signal, and based on its condition and the amount of time the signal took to return, determines cable imperfections. In the case of a coaxial cable network, a TDR can

Not to be reproduced without permission

indicate whether terminators are properly installed and functional. A TDR can also indicate the distance between nodes and segments.

3. Time domain reflectometers are also made for fiber-optic networks. Such instruments are called optical time domain reflectors (OTDRs). Rather than issuing an electrical signal, OTDRs issue a light-based signal over the fiber. Based on the type of return light signal, the OTDR can accurately measure the length of the fiber, determine the location of faulty splices, breaks, connectors, or bends, and measure attenuation over the cable.

Picture 7-2 A typical TDR

Software troubleshooting Tools

Once you have ruled out user error and physical connectivity problems (including faulty cabling) in your troubleshooting, a more in-depth analysis of the network may be necessary. Software-based tools that enable you to analyze network traffic include NOS log files, network monitors, and network analyzers. While log files can reveal what has happened on a server, network monitors and analyzers can capture and interpret data traveling across the network.

Network Monitors

A network monitor is usually a software-based tool that continually monitors traffic on the network from a server or workstation attached to the network. Network monitors typically can interpret up to Layer 3 of the OSI Model. They can determine the protocols passed by each packet, but can't interpret the data inside the packet. By capturing data they can provide either a snapshot of network activity at one point in time or a historical record of network activity over a period of time.

Network monitoring tools are generally less expensive than network analyzers and may be included in your network operating system software. There are two tools that can be part of your network operating system:

Microsoft's Network Monitor (NetMon) is a software-based network monitoring tool that comes with Windows 2000 server. It offers the following capabilities:

- Capturing network data traveling from one or many segments
- Capturing frames sent by or to a specified node
- Reproducing network conditions by transmitting a selected amount and type of data
- Detecting any other running copies of NetMon on the network (depending
- on the placement and configuration of routers)
- Generating statistics about network activity

Network Analyzers

A **network analyzer** (also known as a **protocol analyzer**) is a tool that can capture traffic and analyze packets, typically all the way to Layer 7 of the OSI Model. For example, it can identify that a packet uses TCP/IP. Analyzers can also interpret the payload portion of packets, translating from binary or hexadecimal code to human-readable form. As a result, network analyzers can capture passwords going over the network, if their transmission is not encrypted. Some network analyzer software packages can run on a standard PC, but others require PCs equipped with special network adapters and operating system software.

Troubleshooting TCP/IP

TCP/IP offers several tools that are helpful in the troubleshooting process and provide information to help locate and correct problems. Some of these are listed below:

1. PING - Uses ICMP (Internet control message Protocol) to verify a connection to a remote host by sending echo requests and "listening" for reply packets.

2. ARP - Provides a mapping from the logical 32-bit TCP/IP address to the physical 48-bit MAC address (i.e. translates a IP address into MAC address).

3. TELNET - Provides a virtual terminal or remote login across the network that is connection-based and handles its own session negotiation. The remote server must be running a Telnet service for clients to connect. Defaults settings are Port 23 VT100 terminal emulation.

4. NBTSTAT - Is used to troubleshoot connectivity problems between 2 computers communicating via NetBT, by displaying protocol statistics and current connections. NBTSTAT examines the contents of the NetBIOS name cache and gives MAC address.

5. TRACERT - By sending out ICMP packets, it determines the path taken by a data packet to reach its destination and can help determine at what point a network

Not to be reproduced without permission

connection is no longer active. Can help troubleshoot network response time issues.

6. NETSTAT - Displays in-depth detail about TCP/IP protocol status and statistics.

7. IPCONFIG - Below are the ipconfig switches that can be used at a command prompt.
   - *ipconfig /all* will display all of your IP settings.
   - *ipconfig /renew* forces the DHCP server, if available to renew a lease.
   - *ipconfig /release* forces the release of a lease.

8. NSLOOKUP - This tool queries a DNS database for information about DNS objects and can be used to troubleshoot name **resolution problems**

NetShell (Netsh)

Network Console Shell is a powerful command line utility for viewing and configuring network settings. To use, you type netsh from run. At the netsh prompt if you type ? You will see a list of commands available.

Remote Desktop Overview

With Remote Desktop, you can have access to a Windows session that is running on your computer when you are at another computer. This means, for example, that you can connect to your work computer from home and have access to all of your programs, files, and network resources as though you were sitting at your computer at work. You can leave programs running at work and when you get home, you can see your work desktop displayed on your home computer, with the same programs running.

When you connect to your computer at work, Remote Desktop automatically locks that computer so that no one else can access your programs and files while you are gone. When you come back to work, you can unlock your computer by pressing CTRL+ALT+DEL. You can keep your programs running and preserve the state of your Windows session while another user is logged on. When that user logs off, you can reconnect to your session in progress.

Remote Desktop can be used in many situations, including:

- **Working at home.** Access work in progress on your office computer from home, and have full access to all local and remote devices.
- **Collaborating.** Access your desktop from a colleague's office to work together on projects such as updating a slide presentation or proofreading a document.
- **Maintaining and configuring software**. Change hardware and driver settings, configure software, printer settings etc.

To use Remote Desktop, you need:

- A computer ("host" computer) running Windows XP Professional with Service Pack 2 or Windows Server 2003 with Service Pack 2 ("remote" computer) with a connection to a local area network (LAN) or the Internet.
- A second computer ("client" computer) with access to the LAN via a network connection, modem, or virtual private network (VPN) connection. This computer must have Remote Desktop Connection installed.
- Appropriate user accounts and permissions. (**User name and password**) must be used

Notes:

1. Terminal Services clients use TCP port 3389 to communicate with the remote computer, so you must ensure that this port is not blocked by a firewall.

2. When a remote desktop session to a Microsoft Windows XP Professional computer is started, the console session of the target computer appears as though it has restarted and the active session has been disconnected. This is not the case. The console session is now being displayed remotely on another computer as the remote desktop session.

Reason: Windows XP Professional only allows one connection to the computer at a time. Invoking a remote desktop session when a console session is active will disconnect the console session until you log off or disconnect. The converse is also true: invoking a console session when a remote.

REVIEW QUESTIONS

1. If, after several tries, you cannot reproduce symptoms of a problem, what might you suspect as the cause of the problem?

   a. user error

   b. faulty cabling

   c. incorrect software configuration

   d. incompatible protocols

   e. an improperly installed NIC

Not to be reproduced without permission

2. Which of the following symptoms probably points to a physical connectivity problem?

   a. a group of users consistently experiences delays on the network

   b. a user always loses his drive mappings to file server directories

   c. a group of users complain that they cannot log onto the network

   d. a user can send e-mail but can't pick it up

   e. a user is receiving instant network messages intended for someone else

3. Which part of the network should you examine if a network problem affects a single workstation?

   a. the segment's router interface

   b. the cabling between the switch and the backbone

   c. the workgroup's hub

   d. the workstation's NIC and cabling

4. Answering which two of the following questions may help you identify the demographic scope of a problem?

   a. When did the problem first occur?

   b. How frequently does the problem occur?

   c. How many users have similar symptoms?

   d. Do the symptoms appear on all workstations in one department?

   e. Are the cables properly inserted into the hub, wall jack, and device NIC?

5. Which of the following tools could you use to determine whether a user's workstation is transmitting packets in the proper Ethernet frame type for your network?

   a. multimeter

   b. cable checker

   c. time domain reflector

   d. cable tester

   e. network analyzer

Not to be reproduced without permission

6. What kind of tool would you use to verify that your new cable meets CAT5e standards?

   a. cable tester

   b. cable checker

   c. cable monitor

   d. tone generator and tone locator

   e. multimeter

7. Which TCP/IP command can you use to find out whether a workstation's TCP/IP stack is operating properly?

   a. netstat

   b. nbtstat

   c. ftp

   d. ping

   e. nslookup

8. Where is crosstalk most likely to occur?_____

   _____

   _____

9. If you wanted to determine the average daily traffic on your network's backbone, what type of tool would you use?

   a. network analyzer

   b. cable tester

   c. time domain reflector

   d. network monitor

   e. multimeter

Not to be reproduced without permission

10. Which two of the following functions can both network monitors and network analyzers perform?

    a. capture and analyze data traveling from one node to another

    b. identify a faulty cable

    c. provide trend information on data traffic from a switch port

    d. capture and interpret unencrypted passwords on the network

    e. discover nodes on the network

11. You have just purchased a new network adapter to replace the faulty network adapter in your file server. The adapter is so new that your Windows 2016 Server software does not provide a device driver for it. As you install the network adapter, where should you obtain the device driver from?

    a. the Windows 2016 Server technical support Web site

    b. the network adapter manufacturer's Web site

    c. the disk that came with the network adapter

    d. a server directory containing device drivers for other network adapters used on your network

    e. a client on the network that uses the same network adapter

Not to be reproduced without permission

Skill Practice 7A

Using TCP/IP Diagnostic Tools

Task

To use built in diagnostic tools in a Windows Network

Equipment

- Functional computer with Windows installed.

Procedure

Part A

1. Using PING.

Go to the command prompt: Start / search type cmd , select command prompt.

A. Type ping 127.0.0.1 (loopback test)

Record

Number of packets sent	
Number of packets received	
Number of packets lost	
Time taken	

B. Type ping 192.168.0.40 or another number as specified by the teacher.

In this test you are pinging another machine on the network. If you don't get a reply ask teacher for another IP address.

Record

Number of packets sent	
Number of packets received	
Number of packets lost	
Time taken	

Not to be reproduced without permission

C. Type ping 192.168.0.254 (or other as indicated y the teacher) (node not on network)

Record results.

_____

Why do you think you received this message?

_____

_____

2. Using IPCONFIG.

a. At the command prompt type ipconfig

Record displayed information

b. Type ipconfig /all

Observe results

What is the physical network address of NIC

_____

What is the address on the DNS Server (if applicable)

_____

3. Type hostname at prompt.

Record name (This is the name of your computer) _____

4.. Using Netstat to display protocol statistics

Boot into Windows XP and go to command prompt.

Type netstat ? This will display all the switches associated with netstat.

Try some of the switches eg: netstat –a , netstat –e , netstat –no

Not to be reproduced without permission

Display the routing table; type netstat -nr

Display open ports; type netstat -anop TCP

How many ports are displayed as being open? _____

5. Using Nslookup (**This doesn't work with TAFE proxy settings, will work on most other networks)**

CONNECT TO THE INTERNET

Go to command prompt (type cmd in RUN box)

Type nslookup

What is displayed

_____

_____

Press control c to exit

Type nslookup www.google.com

What is IP address of Google ?_____

Type nslookup bigpond.com

What is IP address of bigpond? _____

To find out IP address of other sites , just enter their address after nslookup.

6. Type arp at command prompt.

A list will be displayed

Find out which switch is needed to display the physical address of the network card. Write down command and the actual physical address.

_____

Try some of the other switches and observe results.

7. In Windows type **netsh** at the RUN command. At the prompt type **?**

A list of commands are displayed.

8. Type **diag** and press enter. Type **?** To display commands. Type **ping adapter** This will ping your adapter card. Type **ping ip** , this will ping your current ip address. Try some of the other commands and look at results.

Not to be reproduced without permission

9. To go back to netsh type **..**

10. Exit program type **bye**

End of practical exercise 7A.

Skill Practice 7B

Using Remote Desktop Connection

Task

To use Remote Desktop Connection to log onto a host PC and make changes

Equipment

- Functional computer with Windows XP installed.

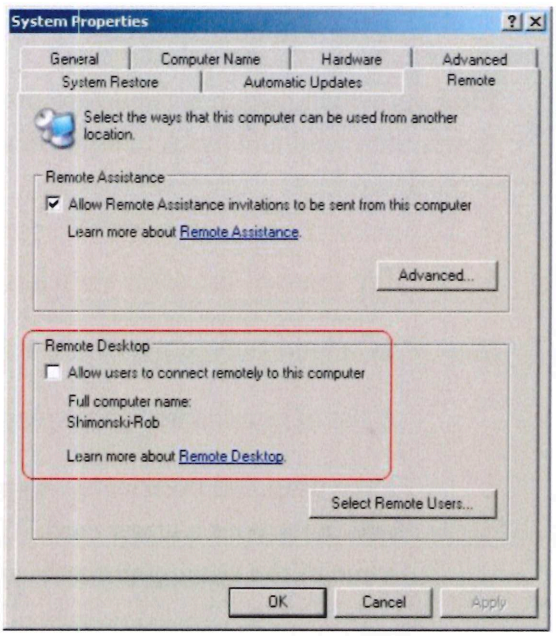
Procedure

You must ***work with the student next to you!***

You must use a user name and password to allow you to use remote desktop. If you didn't log on to PC with a user name and password you will need to create one through the user accounts menu in the control panel. Use student as the user name and student as the password. (lowercase)

1. Check to see if Remote Desktop is installed on both PC's

- The Remote Desktop Connection software is pre-installed with Windows XP so to verify that you have it, use the following :
- Start => All Programs => Accessories => Communications, => Remote Desktop Connection



The Remote Desktop Connection software can be installed on any supported Windows platform. Once you get it, install it and open it up.

Let's look at how to install Remote Desktop (if not already installed. It should be setup on the TAFE computers)

2. Enable Your Computer as the Host

Before you use Remote Desktop, your systems have to be set up properly to allow it to be 'controlled'. One of the first things you will need to do is to 'enable' the remote control of a system. To do that, you will need to make a quick setting change in the System

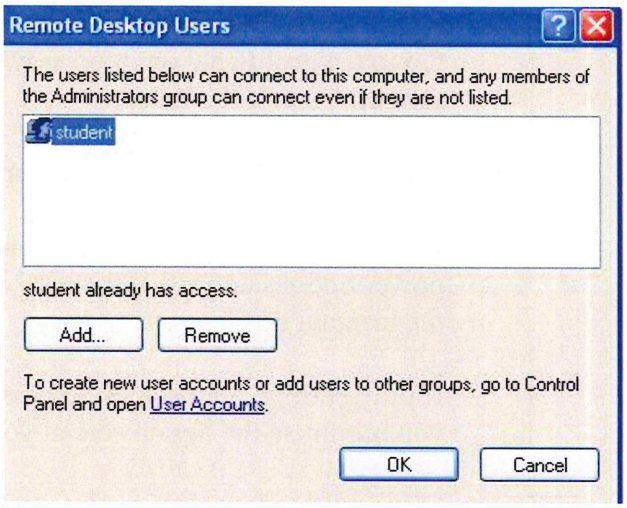
Not to be reproduced without permission

Properties.

1. Log in as an Administrator (or as a member of the Administrators group. The"student" logon has administrator rights)
2. Open the System Applet in the Control Panel.
3. Click Start => Control Panel => System Applet => Remote Tab

4. On the Remote tab, select the Allow users to connect remotely to this computer check box, as shown.
5. Use Select Remote Users tab and add a user (if "student" doesn't appear). Click on Add, then Advanced, then Find Now- select required name from list (student)- Click OK then OK again. The name should appear in the list.

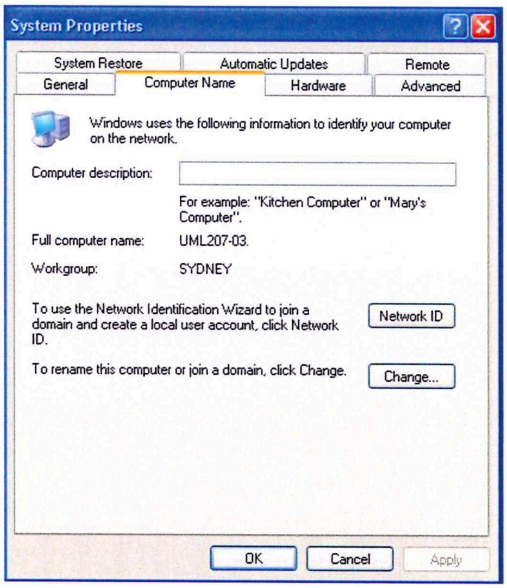
6. Make sure that you have the proper permissions to connect to a computer remotely, and click OK.



Once you have enabled your Windows XP Professional computer to allow remote connections, and installed client software on a Windows-based client computer, you are ready to start a Remote Desktop session.

To create a new Remote Desktop Connection

1. Open Remote Desktop Connection.
2. Click Start => All Programs => Accessories => Communications => Remote Desktop Connection
3. In Computer, type the **computer name** or **TCP/IP** address of the **host** you want to control… remember, they have to be 'allowed' to be controlled first. Use the students computer next to you.
4. To find the **computer name** right click on My Computer and select properties. Select computer name tab. Alternatively you can use the IP address found in network properties.
5. Enter user name and password (student : student).
6. Click Connect.



Your request will now be sent to the system you want to connect to. The Log On to Windows dialog box appears.

Not to be reproduced without permission

7. In the Log On to Windows dialog box, type your user name and password, and then click OK.

8 The Remote Desktop window will open and you will see the desktop settings, files, and programs that are the system. The system that is in the corporate network can remain locked and safe while you are now inside it, working on it. Whatever you are doing cannot be seen by someone watching the console.

You should now be displaying the hosts display on your computer.

1. Go to Control Panel on in open window and select Power Options, make note of the turn off time of the HDD. _____.

2. Now change the time to a different setting and apply it.

3. Go to the host machine and log on to it. Notice the control panel is still open. Go to power options and see if the hard drive turn off time has changed. Change it back to the original setting.

4. If time permits log back on to host PC and open an application and observe results. If you minimise the log on screen you will revert to your standard desktop.

5. Close remote logon screen by click on close in top right hand corner, X.

End.

Not to be reproduced without permission

Additional Student Notes:

Not to be reproduced without permission

Skill Practice 5B

Resetting a network card

On all versions of the Windows's operating system, you need a network adapter to connect to the internet through a wired or wireless network.

Sometimes, you might get an error that your network adapter is missing. This can be very frustrating because you won't be able to connect to the internet.

There are some simple fixes you can use to fix this issue, including:

- removing and reinserting your computer battery
- turning off Antivirus and VPN apps
- restarting your computer

But these might not be enough to fix the issue.

TASK

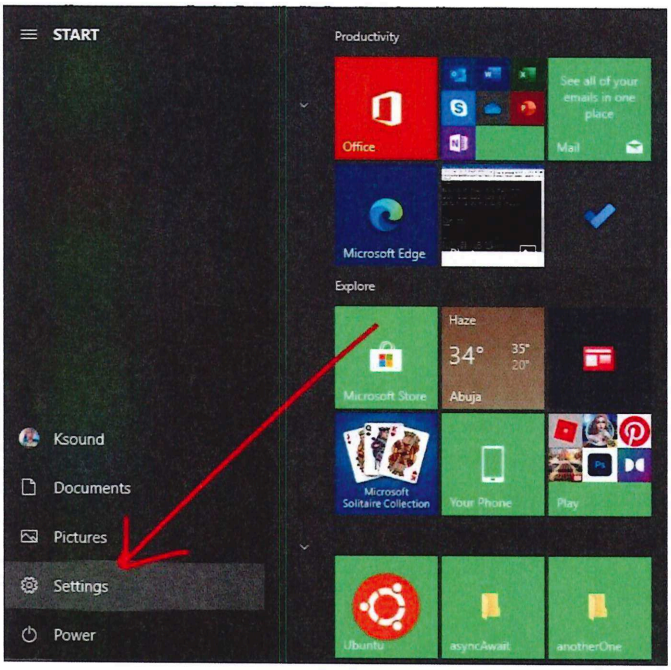
So, in this practical, there are 4 better ways you can fix the network adapter missing error so you can start connecting your computer to the internet again. Work through all five.

1. How to Fix Network Adapter Missing by Using the Built-in Network Reset Tool

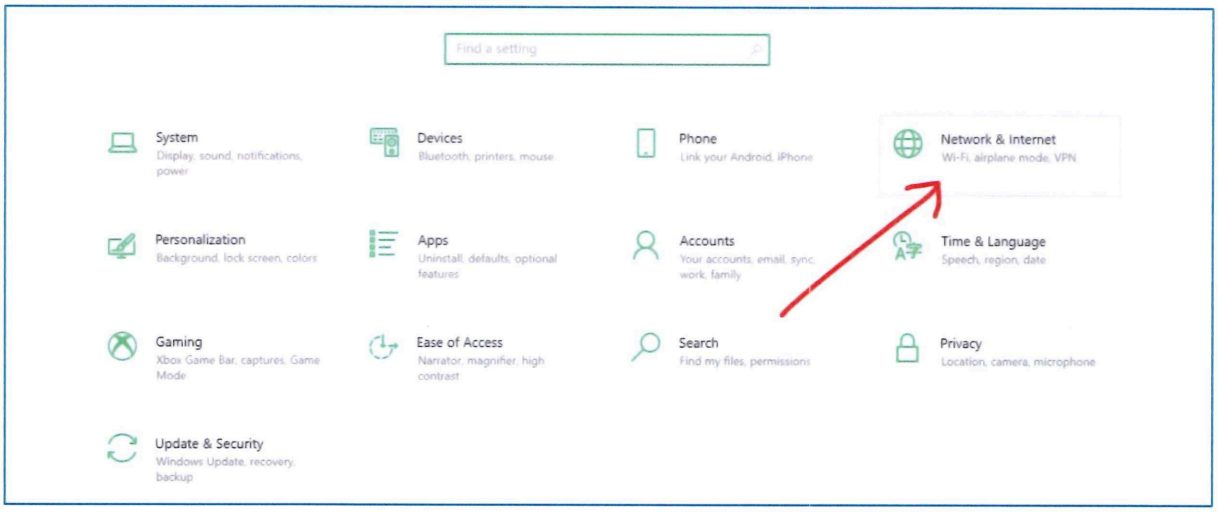
Windows 10 has a built-in network reset tool that can reset your settings to default. This often fixes this issue for you.

To fix the network adapter missing error with this solution, follow the detailed steps below:

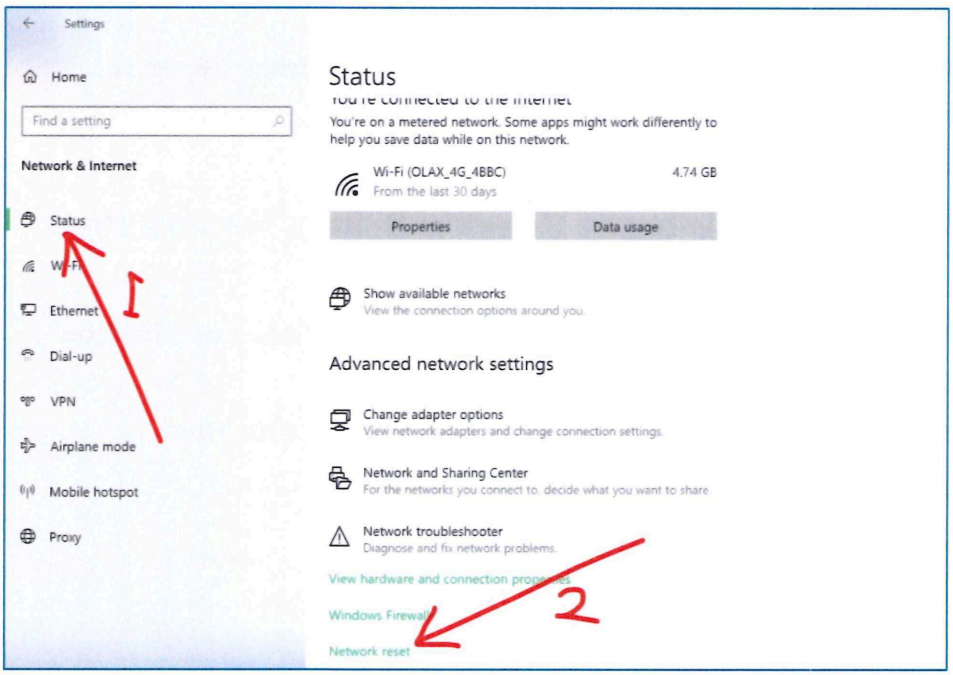
Step 1: Click on Start and select Settings.



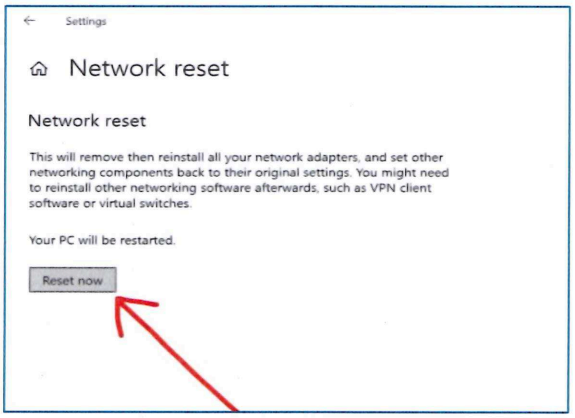
Step 2: Choose Network and Internet from the menu tiles.



Step 3: Under "Status", click the Network reset link.



Step 4: Click the Reset now link.



Note: If you use this fix, be aware that you have to reinstall any VPN app on your computer and also reenter WiFi passwords.

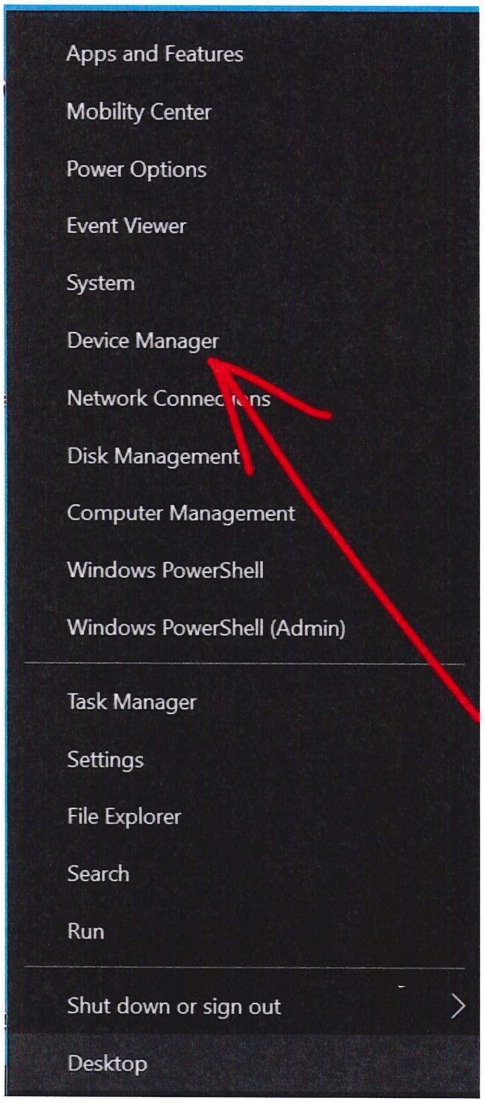
2. How to Fix Network Adapter Missing by Checking the Driver's Power Management Settings

Windows 10 is optimized for better power management, so when your laptop battery is low, some devices could be turned off to save power.

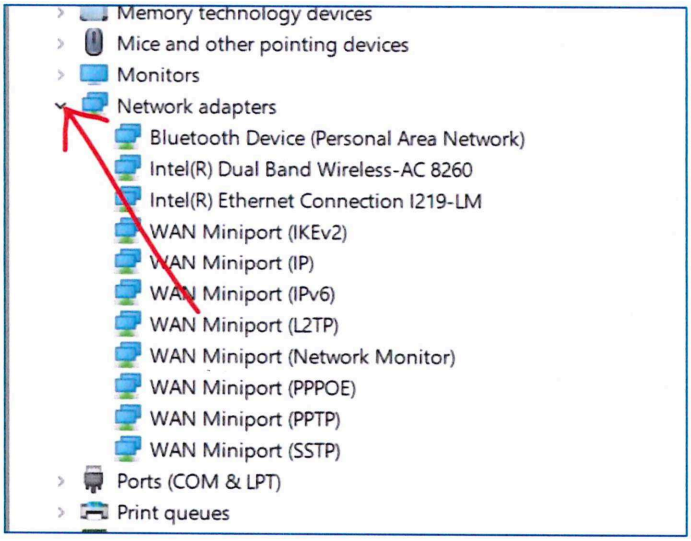
You could experience the network adapter missing error due to this power optimization.

To turn off this feature for your network adapter driver, follow the steps below:

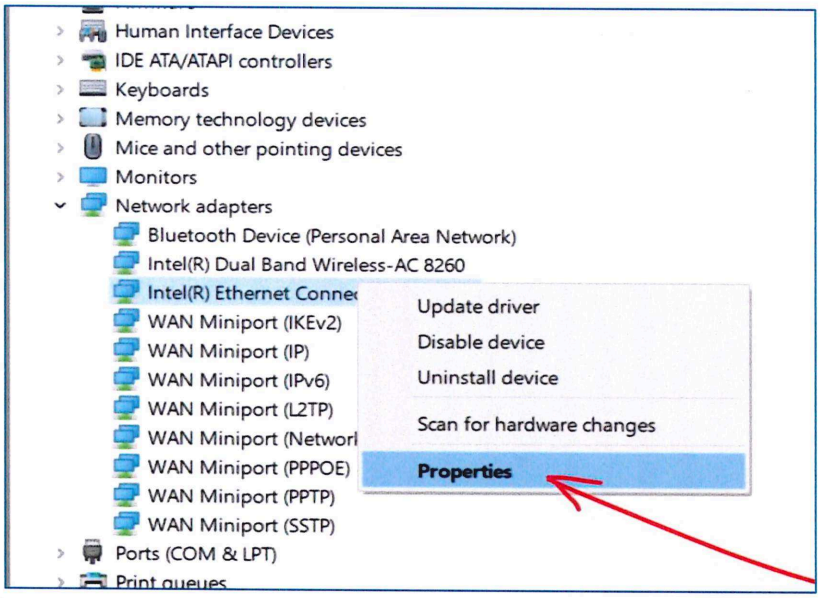
Step 1: Right-click on Start and select Device Manager.



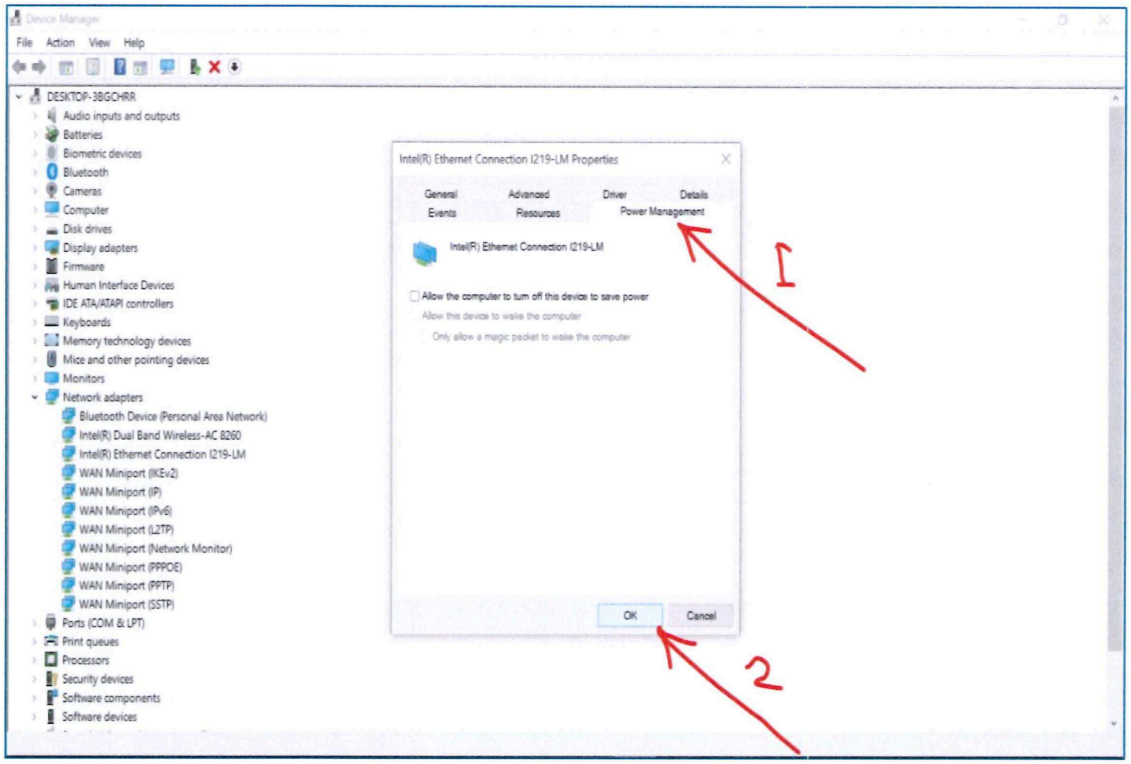
Step 2: Expand Network Adapters.



Step 3: Right-click on the affected network adapter and select Properties.



Step 4: Switch to the Power Management tab and uncheck "Allow the computer to turn off this device to save power" and click "Ok".



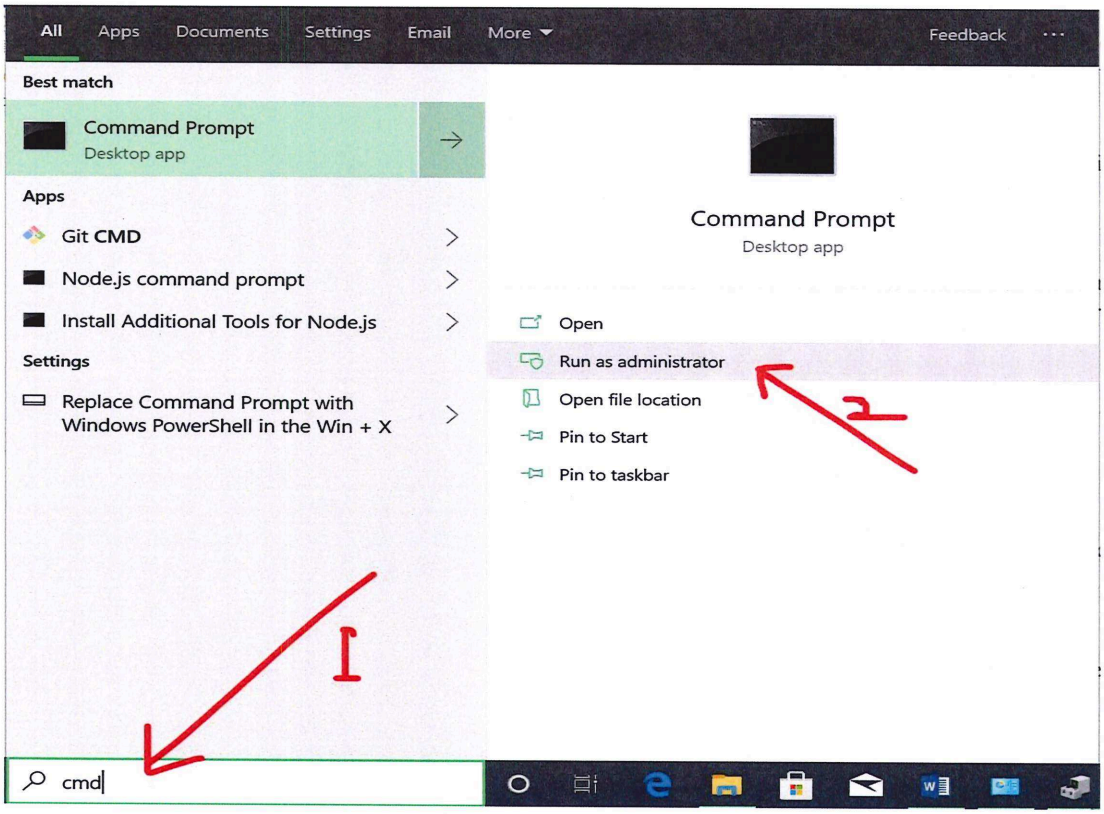
3. How to Fix Network Adapter Missing by Resetting Winsock Settings in the Command Line

Winsock is a program that determines how network services are used on a Windows computer.

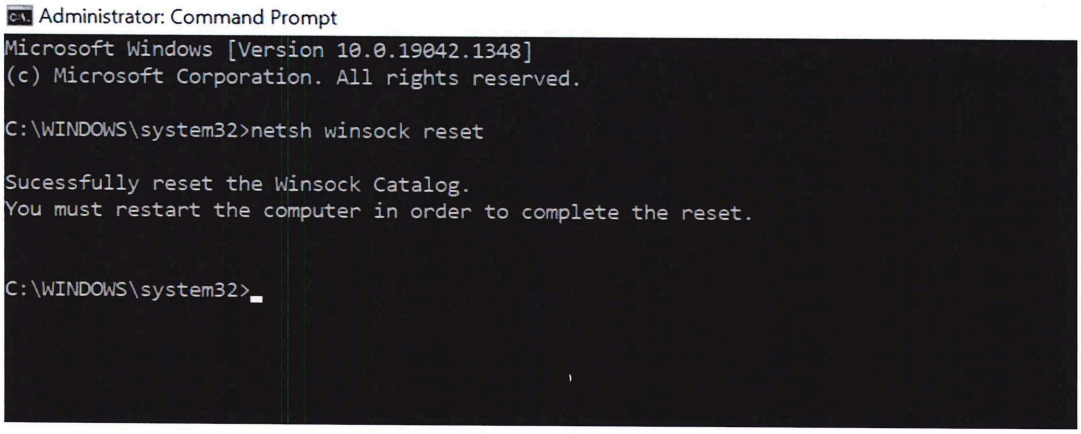
If things go wrong with Winsock, it could cause the network adapter missing error.

To reset Winsock, follow the steps below:

Step 1: Click on Start and search for "cmd", then select "Run as Administrator" on the right.



Step 2: In the command line, type in "netsh winsock reset" and hit ENTER.

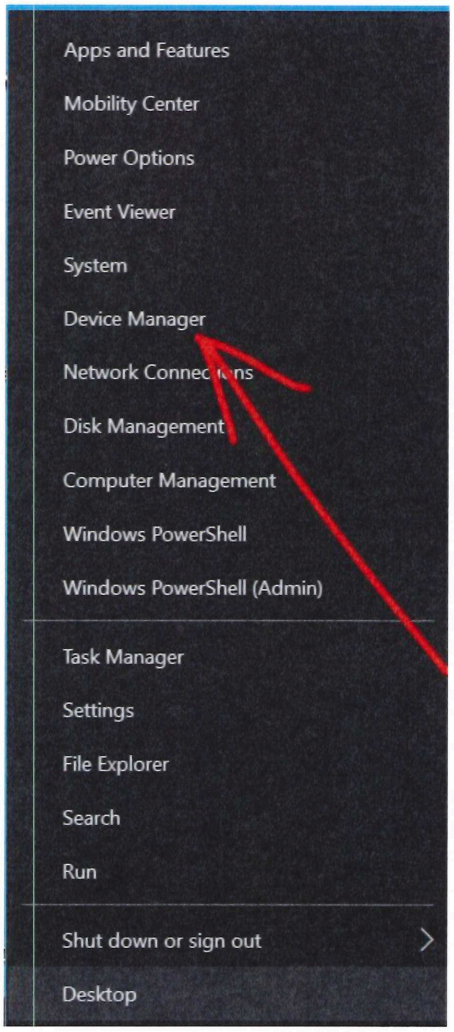


Step 3: Restart your computer.

4. How to Fix Network Adapter Missing by Reinstalling or Updating the Network Adapter Driver

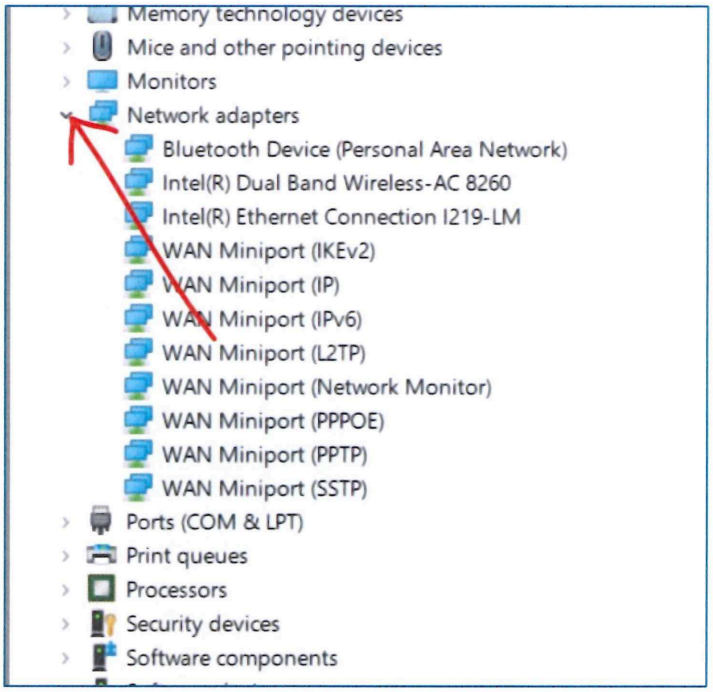
If the solutions already discussed fail to work for your computer, then you should try and reinstall or update your network adapter driver to fix the issue.

To reinstall your network adapter driver, you should follow the steps below:

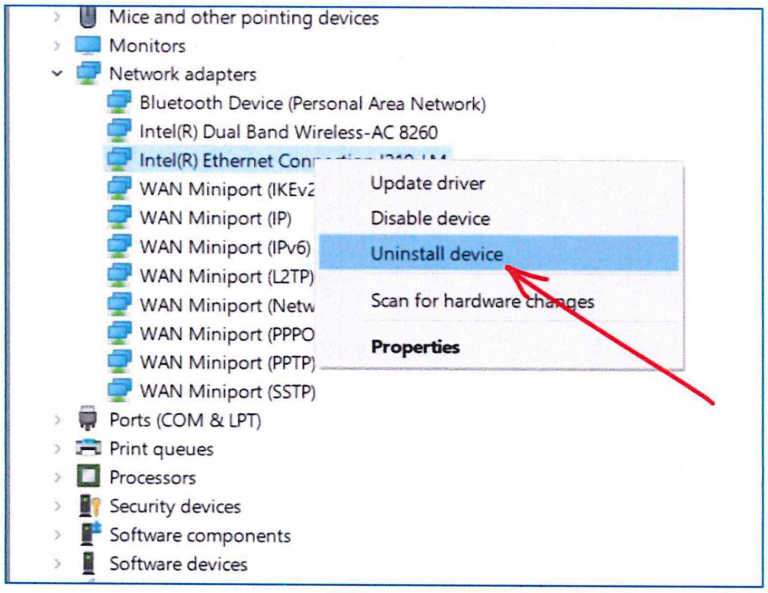


Step 1: Click on Start and select Device Manager.

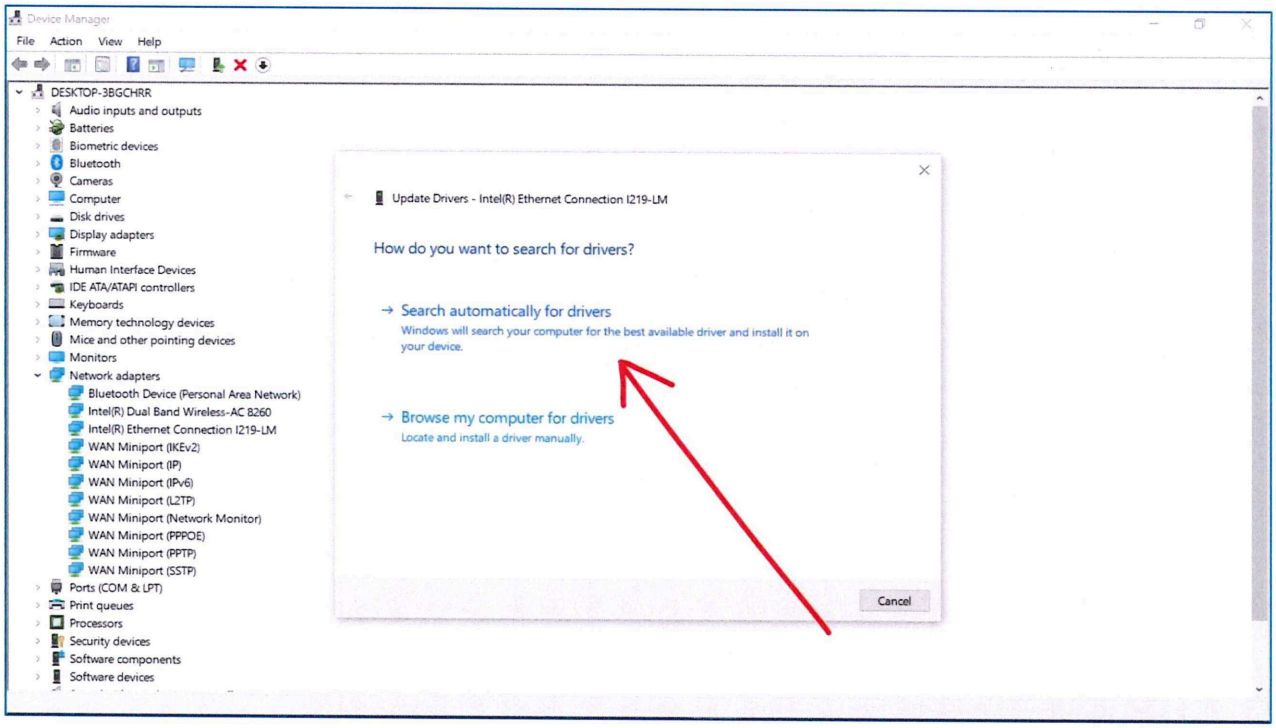
Step 2: Expand Network Adapters.



Step 3: Right-click on the affected driver and select Uninstall device.



Step 4: Choose Search automatically for updated driver software.



Step 5: Restart your computer and the driver will be automatically reinstalled for you.

Conclusion

In this detailed guide, you learned how you can fix the network adapter missing error so you can connect to the internet again with your computer.

If you find this article helpful, consider sharing it with your friends and family so it can help them too.

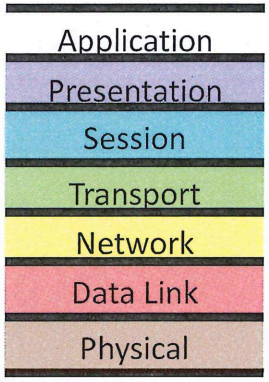
Article from: Chris Kolade, https://www.freecodecamp.org/news/windows-10-network-adapter-missing-how-to-install-ethernet-driver-on-pc/

7-layer OSI model

ISO = International Standardization Organisation
OSI = Open System Interconnection

What does each layer do ?

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical



All People Seem To Need Data Processing

RJ45 Pin	Wire Colour 568A	Wire Diagram 568A	10Base-T Signal 100Base-TX Signal
2	Green		Transmit-
3	White/Orange		Receive+
4	Blue		Unused
5	White/Blue		Unused
6	Orange		Receive-
7	White/Brown		Unused
8	Brown		Unused

Table 1: TIA/EIA 568A pinout colour guide looking from smooth side of connector

RJ45 Pin	Wire Colour 568B	Wire Diagram 568B	10Base-T Signal 100Base-TX Signal
1	White/Orange		Transmit+
2	Orange		Transmit-
3	White/Green		Receive+
4	Blue		Unused
5	White/Blue		Unused
6	Green		Receive-
7	White/Brown		Unused
8	Brown		Unused

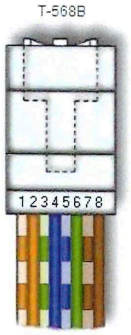


Table 2: TIA/EIA 568B pin out colour guide looking from smooth side of connector

Not to be reproduced without permission